September 15, 2005

Information Technology Management

Report on Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through June 30, 2005 (D-2005-106)

Department of Defense
Office of Inspector General

Constitution of
the United States

A Regular Statement of Account of the Receipts and Expenditures of all public Money shall be published from time to time.

Article I, Section 9

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **15 SEP 2005**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Information Technology Management: Report on Defense Information Systems Agency, Center for Computing Services Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 Through June 30, 2005**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Office of the Inspector General 400 Army Navy Drive Arlington, VA 22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**87**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

September 15, 2005

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFER
ASSISTANT SECRETARY OF DEFENSE (NETWORKS
AND INFORMATION INTEGRATION)/DOD CHIEF
INFORMATION OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Report on Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through June 30, 2005 (D-2005-106)

We are providing this report for your information and use. No written response to this report is required. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Michael Perkins at (703) 325-3557 (DSN 221-3557) or Sean J. Keaney at (703) 428-1448 (DSN 328-1448). The audit team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Patricia A. Marsh
for Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Table of Contents

FOREWARD

This report is intended for the use of Defense Finance and Accounting Service (DFAS) and Defense Information Systems Agency (DISA) management, its user organizations, and the independent auditors of its user organizations. DoD personnel who manage and use the Defense Civilian Pay System (DCPS) will also find this report of interest as it contains information about DCPS general and application controls.

DCPS is a pay processing system used to pay DoD civilian employees, as well as employees at several other Federal entities, including the Departments of Energy and Health and Human Services, and the Executive Office of the President. In 2004, DCPS processed approximately $42.3 billion of pay transactions and paid approximately 762,000 employees on a bi-weekly basis.

The DoD Office of Inspector General (DoD OIG) is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officers Act of 1990 (P.L. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information in DCPS directly impacts the Defense Department's ability to provide reliable, and ultimately auditable, financial statements; which is key to achieving the goals of the Chief Financial Officers Act.

This audit assessed the application and general computer controls over DCPS and its related processing. Those application and general computer controls are managed and maintained by DFAS and DISA. This report provides an opinion on the fairness of presentation, the adequacy of design, and the operating effectiveness of key application and general computer controls that are relevant to audits of user organization financial statements. As a result, this audit precludes the need for multiple audits of DCPS controls previously performed by user organizations to plan or conduct financial statement and performance audits. This audit will also provide, in a separate audit report, recommendations to management for correction of identified control deficiencies. Effective internal control is critical to achieving reliable information for all management reporting and decision making purposes.

Certain DCPS general computer controls are maintained by DISA-Mechanicsburg. DISA-Mechanicsburg was included in the scope of a separate DISA-wide general computer controls audit that provided a Service Auditor's Report, Report No. D-2005-105, "Report on Defense Information Systems Agency, Center for Computing Services Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through April 30, 2005," September 6, 2005. This DISA-wide audit included certain general computer controls that were directly related to DCPS. In order to reduce duplication of effort and minimize the audit footprint on DISA, the DCPS-related general computer controls maintained by DISA-Mechanicsburg and covered by the DISA-wide audit were excluded from the scope of this SAS 70 audit. The control objectives that were not covered for DISA-Mechanicsburg as part of this audit included:

- Control Objective 1: Risks are periodically assessed.

- Control Objective 3: A security management structure has been established and that Information security responsibilities are clearly assigned and expected behavior of all personnel is in place.

- Control Objective 20: Passwords, tokens, or other devices are used to identify and authenticate users.

- Control Objective 46: Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.

- Control Objective 58: Access authorizations are appropriately limited.

- Control Objective 62: Incompatible duties have been identified and policies implemented to segregate these duties.

- Control Objective 63: System management job descriptions have been documented.

- Control Objective 64: System management employees understand their duties and responsibilities.

- Control Objective 65: Management reviews effectiveness of control techniques.

- Control Objective 66: Formal procedures guide system management personnel in performing their duties.

- Control Objective 68: Active supervision and review are provided for all system management personnel.

Certain control objectives listed above were still relevant to other locations included in the scope of this DCPS audit (for example, the Technology Services Organization [TSO]) and are included in this report for those locations. In certain situations where the above control objective would only apply to DISA-Mechanicsburg and was not tested, we inserted "Control objective left intentionally blank" in order to preserve our control objective numbering scheme. User organizations and their auditors who use this report as part of their audit planning procedures should also read the Report No. D-2005-105, "Report on Defense Information Systems Agency, Center for Computing Services Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through April 30, 2005," September 6, 2005 to understand the design and operating effectiveness of the general computer controls maintained by DISA-Mechanicsburg.

Section I: Independent Service Auditor’s Report

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

September 15, 2005

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFER
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND INFORMATION INTEGRATION)/DOD CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through June 30, 2005

We have examined the accompanying description of the general computer and application controls related to the Defense Civilian Pay System (DCPS) (Section II). DCPS is sponsored and used by the Defense Finance and Accounting Service (DFAS) and maintained and technically supported by the Defense Information Systems Agency (DISA) and technical support elements of DFAS. As such, the DCPS general computer and application controls are managed by both DISA and DFAS. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the controls at DFAS and DISA that may be relevant to a DCPS user organization's internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied those aspects of internal controls contemplated in the design of the controls at DFAS and DISA; and (3) such controls had been placed in operation as of June 30, 2005.

The control objectives were specified by the Department of Defense Office of Inspector General (DoD OIG). Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description includes only those application control objectives and related controls resident at the Charleston, SC; Pensacola, FL; and Denver, CO payroll offices and does not include application control objectives and related controls at the National Security Agency (NSA) payroll office. In addition, DCPS processes approximately 140 interface files from DoD and external systems. Examples of these interface systems include the Defense Civilian Personnel Data System, Automated Time and Attendance and Production System, Automated Disbursing System, and the Defense Joint Accounting System. The accompanying description does not include control objectives and general and application controls related to the systems that interface with DCPS. Our examination did not extend to the controls resident at the National Security Agency payroll office and related systems that interface with DCPS.

Our examination was conducted for the purpose of forming an opinion on the description of the DCPS general and application controls at DFAS and DISA (Section II). Information about business continuity plans and procedures at DFAS and DISA, as provided by those organizations and included in Section IV, is presented to provide additional information to user organizations and is not a part of the description of controls at DFAS and DISA. The information in Section IV has not been subjected to the procedures applied in the examination of the aforementioned description of the controls at DFAS and DISA related to their business continuity plans and procedures and, accordingly, we express no opinion on the description of the business continuity plans and procedures provided by DFAS and DISA.

As discussed in the accompanying "Description of DCPS Operations and Controls Provided by DFAS and DISA" (Section II), DISA-Mechanicsburg has processes in place for testing and implementing system software changes. System software change testing results were not required to be documented and maintained. In addition, the charter for the local Configuration Control Board at DISA-Mechanicsburg was not approved. As a result, the design of the controls did not provide reasonable assurance that the control objective "*system software changes are authorized, tested, and approved and documented before implementation*" would be achieved.

In our opinion, the accompanying description of the general computer and application controls at DFAS and DISA related to DCPS (Section II) presents fairly, in all material respects, the relevant aspects of the controls at DFAS and DISA that had been placed in operation as of June 30, 2005. Also, in our opinion, the controls, except for the design deficiency referred to in the preceding paragraph, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and users applied those aspects of internal control contemplated in the design of the controls at DFAS and DISA.

In addition to the procedures that we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified controls, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives described in Section III during the period of October 1, 2004 through June 30, 2005. The specific control objectives, controls, and the nature, timing, extent, and results of the tests are documented in Section III. This information has been provided to DCPS user organizations and to their auditors to be taken into consideration, along with information about the user organizations' internal control environments, when making assessments of control risk for such user organizations.

In performing our examination, we identified the following operating effectiveness deficiencies related to the controls described in the "Description of DCPS Operations and Controls Provided by DFAS and DISA" (Section II):

DCPS User Access

The accompanying description includes control activities relating to DFAS processes for providing access to DCPS. For every DCPS user, DFAS required a Systems Access Authorization Request (SAAR) form be completed, indicating the user's access to DCPS and the authorization by an appropriate supervisor granting such access. Upon examining a selection of 45 randomly selected SAAR forms for payroll office users’ access to DCPS, we identified seven SAAR forms where the access granted in DCPS did not match the access authorized on the SAAR form. In addition, one of 45 payroll office user’s SAAR forms selected for testing did not contain a supervisor’s signature. Upon examining a selection of 45 randomly selected SAAR forms for non-payroll office users’ access to DCPS, we identified four SAAR forms where the access granted in DCPS did not match the access authorized on the SAAR form. In addition, four of the 45 non-payroll office users’ SAAR forms could not be located. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of October 1, 2004 through June 30, 2005:

> “C*ontrols provide reasonable assurance that all application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes,”*
>
> *“Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely,” and*
>
> *“Controls provide reasonable assurance that data transmissions in DCPS from* user *organizations are authorized, complete, accurate and secure.*”

<u>DCPS Processing Error Monitoring</u>

The accompanying description includes control activities relating to DFAS procedures for processing errors from interfacing personnel systems. The Personnel Interface Invalid Report (P6606R01) is a key control for monitoring and resolving DCPS interface processing errors. At the DFAS-Denver payroll office, the Personnel Interface Invalid Reports could not be provided for the period October 1, 2004 through March 27, 2005, which represented 18 of the 45 reports randomly selected for testing. Furthermore, one of the 27 Personnel Interface Invalid Reports for the period March 28, 2005 to June 30, 2005 could not be located (leaving 26 reports available for review). The available Personnel Interface Invalid Reports subsequent to March 27, 2005 were examined to determine if the reports were annotated, indicating the report exceptions were resolved. We identified that annotations on 23 of the 26 available Personnel Interface Invalid Reports for the period of March 28, 2005 to June 30, 2005 did not include the corrective actions taken, 18 out of the 26 Personnel Interface Invalid Reports provided were not dated as completed, and 12 of the 26 Personnel Interface Invalid Reports were not initialed as completed. At the DFAS-Charleston payroll office, because of the inability of the document management system that stores electronic copies of the Personnel Interface Invalid Report to allow annotation of the Personnel Interface Invalid Reports, and only a random review of the reports by management (instead of a review of all reports), the audit team concluded that the controls are not in place to ensure that the Personnel Interface Invalid Reports are properly corrected, annotated, and reviewed by supervisors. Therefore, testing of the reports at the DFAS-Charleston Payroll Office was not performed. At the DFAS-Pensacola payroll office, 10 of the 44 Personnel Interface Invalid Reports selected for testing were not available for review. The remaining 34 reports that were reviewed did not always have the final resolution of errors annotated in the report. Without documented evidence of supervisory reviews and actions taken to address items on this report, there is a lack of a documented audit trail related to the use of this report as a control. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of October 1, 2004 through June 30, 2005:

> *"Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely,"*
>
> *"Controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes,"*
>
> *"Controls provide reasonable assurance that fiscal year-end, leave-year-end and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines," and*
>
> *"Controls are reasonable to ensure that transactions from interfacing systems are subjected to the payroll system edits, validations and error-correction procedures."*

DCPS Interfaces

All DCPS interfaces should have a documented Memorandum of Agreement. The Memorandum of Agreement documents key information about an interface, such as impacted parties, interconnection requirements, points of contact, security requirements, technical platform information, interface file information, and designated signatories. However, 43 out of 148 DCPS interfaces did not have a documented Memorandum of Agreement in place. As a result, the control objective *"owners determine disposition and sharing of data"* may not have been fully achieved during the period of October 1, 2004 through June 30, 2005.

DCPS System Access

For every DCPS system support user at DISA-Mechanicsburg, DISA required a system access request form (Form DD 2875) to be completed, including the access the user required within DCPS and the appropriate supervisor's authorization granting such access. For four out of 45 DISA-Mechanicsburg personnel haphazardly selected for testing, justification for access was not detailed on the system access request form. As a result, the control objective *"access settings have been implemented in accordance with the access authorizations established by the resource owners"* may not have been fully achieved during the period of October 1, 2004 through June 30, 2005.

DCPS Application Change Controls

Testing of DCPS application changes are required to be documented. Testing documentation for 47 of 50 sampled items selected for testing could not be provided by DFAS during the audit. As a result, the control objective *"changes are controlled as programs progress through testing to final approval to ensure completeness, authorization, software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives"* may not have been fully achieved during the period of October 1, 2004 through June 30, 2005.

In our opinion, except for the deficiencies in operating effectiveness noted in the preceding paragraphs, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period of October 1, 2004 through June 30, 2005. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Section III were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Section III.

The relative effectiveness and significance of specific controls at DFAS and DISA, and their effect on assessments of control risk at user organizations, are dependent on their interaction with the internal control environment and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of internal controls placed in operation at individual user organizations.

The description of the controls at DFAS and DISA is as of June 30, 2005, and information about tests of their operating effectiveness covers the period of October 1, 2004 through June 30, 2005. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at DFAS and DISA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that: (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by DCPS management, its user organizations, and the independent auditors of such user organizations.

By direction of the Deputy Inspector General for Auditing:

Patricia A. Marsh
for Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Section II: Description of DCPS Operations and Controls Provided by DFAS and DISA

II. Description of DCPS Operations and Controls Provided by DFAS and DISA

A. Overview of DCPS

Purpose of DCPS

In 1991, the DoD selected DCPS to serve as its standard payroll system for use by all DoD activities paying civilian employees, except Local Nationals and those funded by Non-appropriated Funds and Civilian Mariners. Before becoming the DoD-wide civilian pay system, DCPS was the Navy civilian pay system, which had been in operation since 1988. From a life cycle perspective, DCPS is in the maintenance phase, with changes mainly being driven by legislative and functional enhancements. The DCPS program mission is to process payroll for DoD civilian employees in accordance with existing regulatory, statutory, and financial information requirements relating to civilian pay entitlements and applicable policies and procedures. The DoD civilian pay program must satisfy the complex and extensive functional, technical, and interface requirements associated with the DoD civilian pay function. The functional areas include: employee data maintenance; time and attendance; leave; pay processing; deductions; retirement processing; debt collection; special actions; disbursing and collection; reports processing and reconciliation; and record maintenance and retention. DCPS provides standard interface support to various accounting, financial management, and personnel systems.

DCPS began paying the Executive Office of the President (EOP) in 1998. As part of the President's Management Agenda e-Payroll initiative, DFAS was selected as one of four federal payroll providers to service the entire executive branch of the Federal government. DFAS began processing payroll for the Department of Energy (DOE) in 2003 and the Department of Health and Human Services (HHS) in 2005. DCPS currently processes pay for approximately 762,000 employees.

DCPS is used primarily by approximately 350 payroll processing personnel at three DFAS payroll offices located in Pensacola, FL; Charleston, SC, and Denver, CO. DCPS is also used by NSA[1]. Additional users are the Customer Service Representatives (CSRs) at customer activities and sites. Payroll for DoD civilians is processed by all three DFAS payroll offices. The EOP payroll is processed by the Pensacola payroll office and the DOE and HHS payrolls are processed by the Charleston payroll office.

DCPS Support Functions

The DFAS Military and Civilian Pay Services (M&CPS) Business Line (under the cognizance of the DFAS Director) provides high-level management control and coordination within DoD and for external customers. The Civilian Pay Services Product Line (within the M&CPS) has overall daily responsibility for application, operation, interpretation and implementation of DCPS, as well as responsibility for coordinating with external users and new customers. These responsibilities include requirements management, functional analysis, information assurance, and user documentation processes. The system is maintained and executed on the DISA mainframe platform at

[1] The NSA payroll office is not included in the scope of this "Description of DCPS Operations and Controls Provided by DFAS and DISA".

the Defense Enterprise Computing Center, Mechanicsburg, Pennsylvania (DECC MECH)[2]. The Technology Services Engineering Organization in Pensacola (TSOPE) provides DCPS software engineering and operations support. Within TSOPE, several groups provide DCPS support. The Software Engineering Division provides technical design, programming, unit testing, and system documentation. Integration testing and evaluation processes are performed within the Software Test and Evaluation Division. Project Support provides system software, telecommunication, computer resource tools, and database support. DCPS Software Quality Assurance monitors the software engineering process and provides recommendations for improvement. The Systems Management Directorate provides configuration management, release management, implementation status, and customer support.

DCPS Systems Architecture

DCPS has a two-tiered architecture comprised of the following:

- *Mainframe hardware and software components* - used as a repository for the collection and accumulation of data, and to provide centralized, biweekly processing of civilian pay and its attendant functions (e.g., electronic funds transfer, generation of leave, and earnings statements).

- *Remote user/print spooler hardware and software* - used to collect and/or pre-process data at customer sites, provide connectivity to DCPS mainframe components, and support printing of mainframe generated outputs (e.g., reports, timesheets) at customer locations. These components are largely customer-owned and operated, and include local area networks (LANs), personal computers, and a diverse assortment of printers and software that operates and connects them. A limited number of mid-tier (minicomputer) systems have been maintained by DFAS at selected DFAS sites to handle specialized printing requirements (e.g., paychecks). Other offloaded print services, such as bulk printing for DCPS payroll offices and printing of Leave and Earnings Statements, are performed on PC/workstation hardware maintained by the Defense Automated Printing Service (DAPS) at sites located in various U.S. and overseas geographical regions.

The two tiers of the DCPS architecture are connected via DoD-maintained networks comprised of Internet Protocol (IP)-based (e.g., Non-Classified Internet Protocol Router Network (NIPRNET)) and Systems Network Architecture (SNA)-based (leased line) services. These networks connect DCPS to a wide variety of external, non-DCPS sites (mainframes, mid-tiers, and PCs) that supply or exchange data with DCPS on a regular basis, mainly through electronic file transfers. Examples of external interface sites include the Defense Civilian Personnel Data System, Federal Reserve Board, Thrift Savings Plan, Department of Treasury, and non-DoD users such as DOE, HHS and EOP.

[2] According to DISA, Mechanicsburg is currently a DECC until September 2, 2005. Effective September 3, 2005, all DECCs are being converted to Systems Management Centers.

The main technical components of DCPS include the following attributes:

- DCPS is housed in a separate logical domain on an IBM Z900 mainframe computer located at DECC MECH;

- The IBM mainframe operating system software is Z/OS release 1.4;

- DCPS is written in COBOL II language;

- First point of entry security protection mechanisms are provided by Access Control Facility 2 (ACF2);

- DECC MECH provides four web servers that service all applications that support DCPS. These servers accept the users' secure web requests by supplying a menu screen with options for each application to the DCPS LOGON SCREEN, where individuals enter their ACF2 login user IDs and passwords; and

- Third-party software packages are used for DCPS process scheduling and monitoring.

The payroll offices and associated CSRs have access to DCPS via dedicated leased lines, various DoD networks, and through Secure Web Access. Secure Web Access enables secure transaction processing across the NIPRNET. IBM's Host On Demand was used to establish the Secure Web Access infrastructure. DCPS users interact directly with the DCPS application through "3270" emulation using Personal Computer/Advanced Technology keyboard mapping terminals or terminal simulation programs for communication with DCPS. This permits application-defined formatted screens to be displayed with protected static text and unprotected fields for data entry. The payroll offices are structured in accordance with DFAS standard staffing policy and conduct business using standard operating and support procedures. They operate on a 24-hour basis to provide payroll service to customers located in various time zones and are responsible for the full range of pay processing functions and services. As circumstances dictate, the offices serve as back-up operations sites for each other when contingency procedures must be invoked.

DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003 (DoDI 8500.2), outlines specific control requirements that DoD systems should achieve based on their designated Mission Assurance Category (MAC). According to the current DCPS System Security Authorization Agreement (SSAAs) as of June 30, 2005, the MAC level for the DCPS application is "MAC III" and its supporting enclave at DISA-Mechanicsburg is "MAC II".

DCPS Data Flow

Figure 1 below depicts the DCPS data flow as of April 2005:

Figure 1

Error! Not a valid link.

Overview of System Interfaces

DCPS is a combination of on-line and batch programs that support the requirements of a bi-weekly, and in the case of the President, monthly payroll, for over 762,000 civilian employees in the Federal government based on data feeds from numerous personnel, accounting, and time and attendance systems. Transactions to update employee data, adjust leave balances and payments, and report time and attendance may be input daily to spread the online workload and to obtain labor data. However, the focal point of the system is the bi-weekly process. Non bi-weekly process functions occur monthly, quarterly, annually, or as required, and are in support of or a result of, multiple bi-weekly pay cycles. DCPS supports a standard personnel interface, decentralized time and attendance reporting, and the CSR structure.

DCPS accepts input from three primary areas: CSRs, timekeepers, and personnel offices. DCPS receives or creates approximately 140 interface files that, among other functions:

- update personnel information,
- upload time and attendance data,
- download information for checks to be printed,
- report accounting information to Treasury,
- reconcile enrollment information with health care providers, and
- download general accounting information to DoD agencies.

Automatic electronic file transfer directly to and from the host mainframe computer is preferred for input and output file interfaces. Output files are automatically transmitted to sites and activities using common file transfer protocols, via communication lines of files written to magnetic tape at the host (per data in File Transfer Tables). CSRs must provide File Transfer Table data to TSOPE for table updates. For files not automatically transferred, it is the activity’s responsibility to access the host computer to retrieve (“pull”) their output file(s) from the host. It is the responsibility of the activity creating an input interface file for DCPS to deliver it, by whatever means, to the payroll office or the processing center supporting the payroll office. A mutually agreeable schedule between the payroll activity and the submitting activity must be established to ensure timely receipt of data to support DCPS payroll processing. TSOPE is responsible for executing and monitoring the interface processing as well as resolving interfacing processing errors or problems.

B. Control Environment

DCPS Management Oversight

The DFAS M&CPS Business Line (under the cognizance of the DFAS Director) provides high-level management control and coordination within DoD and DCPS external customers. The Civilian Pay Services Product Line (within the M&CPS) has overall daily responsibility for the DCPS system. The DFAS Information and Technology Directorate is responsible for reviewing, approving the overall DCPS security policy and its certification and accreditation plan, and granting DCPS authority to operate. The TSOPE, a unit of DFAS, provides DCPS software engineering, production support, and customer service. The TSOPE reports to the Civilian Pay Services Product Line. DCPS is maintained and executed on DISA mainframe platforms at DECC MECH. DECC MECH is part of the Center for Computing Services within the Global Information Grid Combat Support Directorate, which is a Strategic Business Unit within DISA. DISA and DFAS are Defense Agencies that report to the Office of the Secretary of Defense. DISA support services provided to DCPS are documented in a signed service level agreement between DISA and DFAS. The service level agreement is reviewed and updated by both agencies on an annual basis. Both DFAS and DISA have documented policies and procedures for their respective functions.

Personnel Policies and Procedures

DFAS Payroll Offices and TSOPE

Payroll office employees and contractors are required to review applicable administrative orders, policies, and procedures with the Human Resource Office and must complete appropriate forms to gain access to DFAS systems. New employees must meet with the Information Security (IS) Manager. The IS Manager is responsible for: (1) providing basic systems security awareness training, (2) securing civilians' and contractors' signatures on an Automated Data Processing Security Awareness disclosure, (3) identifying to the employee who their Terminal Area Security Officer (TASO) is and what the TASO responsibilities are, and (4) notifying appropriate personnel to provide access or to immediately terminate employee and/or contractor access to DFAS automated information system resources when an employee and/or contractor are processing-in or processing-out. The payroll offices and TSOPE facilities do not require any specific level of prior security clearance before a candidate can become an employee.

DECC MECH

The security manager is responsible for processing and vetting new employees and contractors who are given access to DISA facilities in Mechanicsburg. All contractors and employees are required, at a minimum, to have a secret clearance and a positive National Agency Check for employees, the security manager coordinates with the personnel office and for contractors, the security manager coordinates with the contracting officer. The contracting officer is responsible for confirming that all contractors are assigned to a valid contract, and have been approved to operate at DECC MECH.

All new employees are required to sign DISA Form 312, ”Classified Information Nondisclosure Agreement,” which serves as a nondisclosure agreement for sensitive and classified information. When employees are terminated, DISA requires them to sign the same Form 312 to confirm their understanding of the requirements put upon them. For new employees and contractors to gain access to DISA systems, they are required to complete DD Form 2875, “System Authorization Access Request.” The security manager is responsible for vetting these forms and confirming that the person requesting access has the proper clearance for the level of access requested. For contractors, the security manager confirms the length of the contract and determines when system accounts should expire. All new employees and contractors must complete security awareness training.

C. Monitoring

Management and supervisory personnel at DFAS and DISA monitor the performance quality and internal control environment as a normal part of their activities. DFAS and DISA have implemented a number of management, financial, and operational reports that help monitor the performance of payroll processing, as well as the DCPS system itself. These reports are reviewed periodically and action is taken as necessary. All procedural problems and exceptions to normal and scheduled processing are logged, reported, and resolved in a timely manner, with remedial action taken as necessary.

In addition, several organizations within DoD perform monitoring activities associated with DCPS-related internal controls. These functions include:

DISA Office of the Inspector General and Field Security Office

DISA has its own Office of Inspector General (OIG), which is an independent office within DISA that conducts internal audits, inspections, and investigations. The DISA-related components that support DCPS are part of the DISA OIG audit universe and are subject to audits, inspections, and investigations conducted by this office.

In addition, DISA has a Field Security Operations (FSO) unit that performs periodic System Readiness Reviews of DISA systems to determine whether those systems are in compliance with the DISA documented Standard Technical Implementation Guides

(STIGs). The DCPS system components that are maintained by DISA are subject to these FSO reviews. The FSO is independent of the DECC MECH management structure and does not maintain or configure DCPS systems.

Certification and Accreditation

DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, establishes a standard Department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems that will maintain the information assurance and security posture of the defense information infrastructure throughout the life cycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards to establish the extent to which a particular design and implementation meets specified security requirements and covers physical, personnel, administrative, information, information systems, and communications security. The accreditation process is a formal declaration by the designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

DCPS is subject to the requirements of DITSCAP and must meet all of the DITSCAP certification and accreditation requirements throughout its life cycle. As part of the DCPS DITSCAP process, separate SSAAs have been prepared for the DCPS application itself and for the system enclave within DISA that supports the application. Each SSAA is a living document that represents an agreement between the designated approving authority, certifying authority, user representative, and program manager. Among other items, the DCPS SSAA documents DCPS' mission description and system identification, environment description, system architecture description, system class, system security requirements, organizations and resources, and DITSCAP plan. On a periodic basis, the system security officer must verify and validate DCPS' compliance with the information in the SSAA. These verification and validation procedures include, among other steps, vulnerability evaluations, security testing and evaluation, penetration testing, and risk management reviews. The DCPS application SSAA, which was issued in May 2002 and valid for three years, is currently being modified as part of their DITSCAP recertification and reaccredidation process that is expected to be completed in July 2005. The DECC MECH enclave SSAA, which was issued in October 2003 is valid for three years and is the same SSAA that was in place for the DCPS audit report issued in October 2004.

DoD Office of Inspector General (DoD OIG)

The DoD OIG was established under the Inspector General Act of 1978 by Congress to conduct and supervise audits and investigations related to the programs and operations of the DoD. The DoD OIG reports directly to the Secretary of Defense and is independent of DFAS and DISA. DCPS, as well as the payroll processes it supports, is part of the DoD OIG audit universe and is subject to financial, operational, and information technology audits, reviews, and special assessment projects.

D. Risk Assessment

The DITSCAP process, discussed in subsection C above, includes several activities that document and assess risks associated with DCPS. The DCPS application and enclave SSAAs, which are a product of the DITSCAP process, also document threats to DCPS and its supporting technical environment. The SSAAs also contain Residual Risk Assessments that document vulnerabilities noted during DCPS tests and analyses. The information contained in the SSAAs is updated on a periodic basis. Personnel from DFAS TSOPE and DECC MECH participate in these risk assessment activities.

E. Information and Communication

DCPS is the information system used to process civilian payroll for DoD and its payroll customers, such as EOP, DOE and HHS. The processing of payroll involves over 140 data files that interface with DCPS. These interfaces are linked to other DoD financial systems as well as external systems. The majority of the interfaces are automated. All automated interfaces must conform to documented interface specifications developed by the TSOPE, who is responsible for executing and monitoring the automated interfaces.

The support relationship between DFAS and DECC MECH is documented through a service level agreement that is reviewed and updated annually. The service level agreement outlines various DFAS and DECC MECH points of contact and liaisons that should be used when DCPS issues arise. DECC MECH also assigned a customer relationship manager to work with DFAS TSOPE to resolve any DCPS processing problems or concerns.

Within DFAS, the TSOPE and payroll offices have a weekly meeting between the directors and managers of both organizations to discuss DCPS processing issues. There is also a Configuration Control Board (CCB), comprised of TSOPE and payroll office personnel, to review and approve functional and systemic changes to DCPS. The payroll offices also have a help desk function to identify and track user issues and problems with DCPS and communicate those issues and problems to the TSOPE for resolution.

F. Control Activities

The DCPS control objectives and related control activities are included in Section III of this report, “Information Provided by the Service Auditor,” to eliminate the redundancy that would result from listing them in this section and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are, nevertheless, an integral part of the description of controls.

G. User Organization Control Considerations

The control activities at DFAS and DISA related to DCPS were designed with the assumption that certain controls would be placed in operation at user organizations. This section describes some of the controls that should be in operation at user organizations to complement the controls at DFAS and DISA.

User organizations should have policies and procedures in place to ensure that:

- The Information Systems Security Officer (ISSO) located at the payroll offices is notified of all terminated employees that are DCPS users.

- The local Human Resource Office is notified of all terminated employees, so that such employees are removed from the Master Employee Record in a timely manner.

- All time entered by timekeepers is approved and authorized by appropriate user organization management.

- All Master Employee Records created represent valid employees.

- All changes to the Master Employee Record are approved by appropriate user organization personnel prior to payroll processing.

- Segregation of duties exists between those at the user organization who enter time and those who enter or change Master Employee Records.

- If a pseudo Social Security Number (SSN) is created, the pseudo SSN has been authorized by appropriate user organization personnel and, if necessary, is accurately tied to a primary and valid SSN.

- User organization managers review the "Control of Hours" and other payroll-related reports for appropriateness and accuracy.

- All invalid time entry interface feeds are reviewed and processed by appropriate user organization personnel in a controlled manner.

- All invalid personnel record interface feeds are resolved in the interface system by user organization personnel with appropriate approval by user organization management.

Section III: Control Objectives, Control Activities, and Tests of Operating Effectiveness

III. Control Objectives, Control Activities, and Tests of Operating Effectiveness

A. Scope Limitations

The control objectives documented in this section were specified by the DoD OIG. As described in the prior section (Section II), DCPS interfaces with many systems. The controls described and tested within this section of the report are limited to those computer systems, operations, and processes directly related to DCPS itself. The controls related to the source and destination systems associated with the DCPS interfaces are specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls within these interface systems. However, we did perform procedures to evaluate DCPS interface input and output controls. In addition, we did not perform any procedures to evaluate the integrity and accuracy of the data contained in DCPS.

B. Control Objectives, Control Activities, and Tests of Operating Effectiveness

Application Control Objectives, Activities, Test Procedures and Results of Testing

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
1	Controls provide reasonable assurance that only valid and accurate changes are made to the payroll master files and payroll withholding tables.	Policies and procedures are documented to describe that only valid and accurate changes are made to the payroll master files and payroll withholding tables.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the processing of valid changes to the payroll master files and payroll existed and were documented.	**No relevant exceptions noted**.
		Payroll master file and withholding data tables are periodically reviewed by supervisory personnel for accuracy and ongoing pertinence.	Inspected Online Queries (OLQs) and Master Employee Add/Change/Delete reports and inquired with appropriate personnel to confirm that master files and withholding tables were periodically reviewed by supervisory personnel for accuracy and ongoing pertinence.	DFAS Charleston The OLQs and Master Employee Add/Change/Delete reports were not signed off on to indicate they have been reviewed. However, as a mitigating circumstance, we observed that the Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.
		Programmed validation and edit checks identify erroneous data.	Observed programmed validation and edit checks and inquired with appropriate personnel and to confirm they existed.	**No relevant exceptions noted.**
		Changes to the payroll withholding tables and master files are compared to authorized source documents by supervisory personnel to ensure that they were input accurately.	Observed the process of tax changes to the payroll withholding tables and master files being compared to authorized source documents by supervisory personnel and inquired with appropriate personnel and to confirm that they were tested and approved. Observed the imaging process to confirm that inputs were compared to authorized imaging documents and inquired with appropriate personnel to	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			confirm that they were input accurately.	
2	Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	Policies and procedures are documented to describe that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the processing of changes to payroll master files and withholding tables existed and were documented.	**No relevant exceptions noted.**
		Changes to the payroll master file and withholding table data are logged in numerous reports including the Master Employee Add/Change/Delete Report and reviewed by supervisory personnel to ensure that all requested changes are processed timely.	Inquired with appropriate personnel and inspected the Master Employee Add/Change/Delete report to confirm that changes to the payroll master file and table data were logged and reviewed by supervisory personnel.	DFAS Charleston The Master Employee Add/Change/Delete reports, as well as other summary reports, were not signed off to indicate they were reviewed. However, as a mitigating circumstance, we observed that the Payroll Office staff reviewed the summary reports and the reports were archived indicating that they had been run.
		Requests to change the payroll master file data and withholding table are submitted on pre-numbered Remedy Tickets; the numerical sequence of the Remedy Tickets is accounted for to ensure that the requested changes are processed timely. Access to source documents is controlled; Key source documents require signatures from supervisory personnel.	Inspected a random sample of 45 Remedy Tickets and inquired with appropriate personnel to confirm the requests: • Were pre-numbered; • That the sequence was accounted for so that the forms were accounted for timely; • That access to the source documents was restricted, and • That key source documents required signatures from supervisory personnel.	DFAS-Denver One of 45 Remedy Tickets tested was not completed within the required timeframe. DFAS-Pensacola Four of 45 Remedy Tickets tested were not completed within the required timeframe. DFAS-Charleston Two of 45 Remedy Tickets tested were not completed within the required time frame.
		Payroll master file data and withholding table data are edited and validated and errors identified on the	Inspected a haphazard sample of 45 Personnel Interface Invalid Reports of erroneous transactions and inquired	DFAS-Denver Due to technical difficulties with the document management system

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Personnel Interface Invalid Report are corrected promptly.	with appropriate personnel to confirm items were investigated and resolved timely.	used to store the Personnel Interface Invalid Reports, the Personnel Interface Invalid Reports could not be provided prior to March 27, 2005, which represented 18 of the 45 reports selected for testing. Additionally, one of the remaining 27 reports from March 28, 2005 through June 30, 2005 could not be located, which left the sample of 26 to be reviewed. Annotations on 23 of the 26 Personnel Interface Invalid Reports from March 28, 2005 through June 30, 2005 did not include the corrective actions taken; 18 out of the 26 Personnel Interface Invalid Reports provided were not dated as completed, and 12 of the 26 Personnel Interface Invalid Reports were not initialed as completed. DFAS-Charleston Due to the inability of the system to allow annotation of the Personnel Interface Invalid Reports and payroll office personnel performed an undocumented random review of the reports instead of a documented review all reports, the audit team could not determine that the Personnel Interface Invalid Reports are properly corrected, annotated, and reviewed by supervisors. Therefore, testing of the reports at DFAS Charleston payroll office was not performed.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				DFAS-Pensacola Ten of the 44 Personnel Interface Invalid Reports were not available for review. The remaining 34 reports that were reviewed did not always have the final resolution of errors annotated in the report. The Personnel Interface Invalid Reports were not reviewed by a supervisor to ensure all exceptions noted on the report had been corrected by the payroll technician.
		The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Inspected a random sample of 45 access forms to confirm the user on the form was properly authorized and that the access granted on the form matched the access granted within DCPS.	Payroll Office Users Seven of 45 payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, one of 45 payroll office user's SAAR forms selected for testing did not contain a supervisor's signature. Non-Payroll Office Users Four of 45 non-payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, four of the 45 non-payroll office users' SAAR forms could not be located.
3	Controls provide reasonable assurance that payroll processing is accurate and recorded in the proper period.	Policies and procedures are documented to describe that payroll processing is accurate and recorded in the proper period.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the accurate processing and recording of payroll existed and were documented.	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Compliance with the payroll disbursement processing schedule is monitored by management.	Observed payroll disbursement processes and inquired with appropriate personnel and inspected pay processing schedules to confirm that management was monitoring the payroll disbursement processing schedule.	**No relevant exceptions noted.**
		The detailed “592” payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, Thrift Savings Plan (TSP), Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inspected a sample of 20 (to include all pay periods during the 9 month audit period) “592” reconciliations for each database and inquired with appropriate personnel to confirm: • The detailed payroll reconciliation showed pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances were reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; • Each “592” reconciliation was approved by management prior to disbursement and; • Reconciling items were investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	**No relevant exceptions noted.**
		Summary payroll reports including OLQs of total disbursements, Retirement, TSP, Bonds, and other withholdings are reviewed and approved by management prior to disbursement.	Inspected summary reports and OLQs, observed payroll office staff summary report and OLQ review procedures, and inquired with appropriate personnel to confirm they were reviewed and approved by	<u>DFAS Charleston</u> The summary reports, including the OLQs, were not signed off on to indicate they were reviewed. However, as a mitigating circumstance, we observed that the

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			management prior to disbursement.	Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.
4	Controls provide reasonable assurance that disbursed payroll (including compensation and withholding) is accurately calculated and recorded.	Policies and procedures are documented to describe that management ensures disbursed payroll (including compensation and withholding) is accurately calculated and recorded.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the disbursement of payroll existed and were documented.	**No relevant exceptions noted.**
		The detailed "592" payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inspected a sample of 20 (to include all pay periods during the 9 month audit period) "592" reconciliations for each database and inquired with appropriate personnel to confirm: • The detailed payroll reconciliation showed pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances were reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; • Each "592" reconciliation was approved by management prior to disbursement and; • Reconciling items were investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	**No relevant exceptions noted.**
		Summary payroll reports including OLQs of total disbursements, Retirement, TSP, Bonds, and other withholdings) are reviewed and	Inspected summary reports and OLQs, observed payroll office staff summary report and OLQ review procedures, and inquired with appropriate	<u>DFAS Charleston</u> The summary reports, including the OLQs, were not signed off to indicate they were reviewed.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		approved by management prior to disbursement.	personnel to confirm they were reviewed and approved by management prior to disbursement.	However, as a mitigating circumstance, we observed that the Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.
		DCPS performs limit and reasonableness checks on employee earnings.	Inspected a report showing earnings limit and reasonableness errors and inquired with appropriate personnel to confirm whether reasonableness checks were performed on employee earnings.	**No relevant exceptions noted.**
		Programmed validation and edit checks identify erroneous data.	Observed the entering of new employee information into DCPS to confirm that programmed validation and edit checks were executed.	**No relevant exceptions noted.**
5	Controls provide reasonable assurance that only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	Policies and procedures are documented to describe that management ensures only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to disbursement of payroll to valid and authorized employees existed and were documented.	**No relevant exceptions noted.**
		OLQs and summary reports such as the Master Employee Add/Change/Delete Report are periodically reviewed by supervisory personnel to determine if the master files remain accurate and pertinent.	Inspected OLQs and Master Employee Add/Change/Delete reports, observed payroll office staff summary report and OLQ review procedures, and inquired with appropriate personnel to confirm that master files and withholding tables were periodically reviewed by supervisory personnel.	DFAS Charleston The OLQs and Master Employee Add/Change/Delete reports were not signed off to indicate they were reviewed. However, as a mitigating circumstance, we observed that the Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.
		Departmental managers periodically review listings, such as the Personnel/Payroll Reconciliation and Control of Hours Report, of current employees within their departments and notify the personnel department of	Inspected the Personnel/Payroll Reconciliation and Control of Hours Reports and inquired with appropriate personnel to confirm they were sent to management for review of employee listings and notification to personnel	**No relevant exceptions noted**.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		necessary changes. All payroll queries are followed up by persons independent of the payroll preparation and disbursement process.	department of changes.	
		The detailed “592” payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inspected a sample of 20 (to include all pay periods during the 9 month audit period) “592” reconciliations for each database and inquired with appropriate personnel and to confirm: • The detailed payroll reconciliation showed pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances were reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; • Each “592” reconciliation was approved by management prior to disbursement and; • Reconciling items were investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	**No relevant exceptions noted.**
		Summary payroll reports including OLQs of total disbursements, Retirement, TSP, Bonds, and other withholdings) are reviewed and approved by management prior to disbursement.	Inspected summary reports and OLQs and inquired with appropriate personnel to confirm they were reviewed and approved by management prior to disbursement.	DFAS Charleston The OLQs and Master Employee Add/Change/Delete reports were not signed off to indicate they were reviewed. However, as a mitigating circumstance, we observed that the Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Only authorized personnel have the ability to disburse payroll.	Observed the disbursement of payroll, inspected a random sample of 45 DCPS users, and inquired with the appropriate personnel to confirm that only authorized personnel had the ability to disburse payroll.	**No relevant exceptions noted.**
6	Controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	Policies and procedures are documented to describe that management ensures controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the controls over the integrity and reliability of DCPS data existed and were documented.	**No relevant exceptions noted.**
		Payroll transactions at the end of a payroll cycle are reconciled by supervisory personnel to ensure complete and consistent recording in the appropriate accounting period.	Inspected a sample of 20 (to include all pay periods during the 9 month audit period) "592" payroll reconciliations at the end of a payroll cycle and inquired with appropriate personnel to confirm they were reconciled.	**No relevant exceptions noted.**
		Error reports, such as the Personnel Interface Invalid Report, and error warnings show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	Inspected error warnings and a haphazard sample of 45 Personnel Interface Invalid Reports and inquired with appropriate personnel to confirm they showed rejected transactions with error messages that had clearly understandable corrective actions for each type of error.	DFAS-Denver Due to technical difficulties with the document management system used to store the Personnel Interface Invalid Reports, the Personnel Interface Invalid Reports could not be provided prior to March 27, 2005, which represented 18 of the 45 reports selected for testing. Additionally, one of the remaining 27 reports from March 28, 2005 through June 30, 2005 could not be located, which left the sample of 26 to be reviewed. Annotations on 23 of the 26 Personnel Interface Invalid Reports from March 28, 2005 through June 30, 2005 did not include the corrective actions taken; 18 out of the 26 Personnel Interface Invalid Reports provided were not

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				dated as completed, and 12 of the 26 Personnel Interface Invalid Reports were not initialed as completed. <u>DFAS-Charleston</u> Due to the inability of the system to allow annotation of the Personnel Interface Invalid Reports and payroll office personnel performed an undocumented random review of the reports instead of a documented review all reports, the audit team could not determine that the Personnel Interface Invalid Reports are properly corrected, annotated, and reviewed by supervisors. Therefore, testing of the reports at DFAS Charleston payroll office was not performed. <u>DFAS-Pensacola</u> Ten of the 44 Personnel Interface Invalid Reports were not available for review. The remaining 34 reports that were reviewed did not always have the final resolution of errors annotated in the report. The Personnel Interface Invalid Reports were not reviewed by a supervisor to ensure all exceptions noted on the report had been corrected by the payroll technician.
		Rejected data are automatically written to the Personnel Interface Invalid Report and held until corrected by payroll technicians, and each erroneous transaction is annotated with codes indicating the type of data	Inspected the Personnel Interface Invalid Report of rejected data and inquired with the appropriate personnel to confirm that the rejected data were automatically written on an automated error suspense file and held	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		error, date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction.	until corrected by payroll technicians. In addition, verified whether each erroneous transaction was annotated with codes indicating the type of data error, date and time the transaction was processed, the error identified, and the identify of the user who originated the transaction.	
7	Controls provide reasonable assurance that fiscal year-end, leave-year-end and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines.	Policies and procedures are documented to describe that management ensures fiscal year-end, leave-year-end and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to fiscal year-end, leave-year-end, and calendar year-end processing existed and were documented.	**No relevant exceptions noted.**
		Payroll withholding table data is periodically reviewed by supervisory personnel for compliance with statutory requirements.	Inspected payroll withholding table data updates to confirm they were periodically updated by supervisory personnel for compliance with statutory requirements.	**No relevant exceptions noted.**
		The detailed "592" payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inquired with appropriate personnel and inspected a sample of 20 (to include all pay periods during the 9 month audit period) "592" reconciliations for each database to confirm: • The detailed payroll reconciliation showed pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances were reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; • Each "592" reconciliation was	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			approved by management prior to disbursement and; • Reconciling items were investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	
		The data processing control group has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; reviews output products for general acceptability; and reconciles control information to determine completeness of processing.	Inspected the schedules used by the data processing group and inquired with appropriate personnel to confirm they: • Had a schedule by application that showed when outputs needed to be completed, when they needed to be distributed, who the recipients were, and the copies needed; • Reviewed output products for general acceptability, and • Reconciled control information to determine completeness of processing.	**No relevant exceptions noted.**
		Users review the Personnel Interface Invalid Reports for data accuracy, validity, and completeness.	Inspected a haphazard sample of 45 Personnel Interface Invalid Reports and inquired with appropriate personnel to confirm the reports were reviewed for data accuracy, validity, and completeness.	<u>DFAS-Denver</u> Due to technical difficulties with the document management system used to store the Personnel Interface Invalid Reports, the Personnel Interface Invalid Reports could not be provided prior to March 27, 2005, which represented 18 of the 45 reports selected for testing. Additionally, one of the remaining 27 reports from March 28, 2005 through June 30, 2005 could not be located, which left the sample of 26 to be reviewed. Annotations on 23 of the 26 Personnel Interface

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				Invalid Reports from March 28, 2005 through June 30, 2005 did not include the corrective actions taken; 18 out of the 26 Personnel Interface Invalid Reports provided were not dated as completed, and 12 of the 26 Personnel Interface Invalid Reports were not initialed as completed. <u>DFAS-Charleston</u> Due to the inability of the system to allow annotation of the Personnel Interface Invalid Reports and payroll office personnel performed an undocumented random review of the reports instead of a documented review all reports, the audit team could not determine that the Personnel Interface Invalid Reports are properly corrected, annotated, and reviewed by supervisors. Therefore, testing of the reports at DFAS Charleston payroll office was not performed. <u>DFAS-Pensacola</u> Ten of the 44 Personnel Interface Invalid Reports were not available for review. The remaining 34 reports that were reviewed did not always have the final resolution of errors annotated in the report. The Personnel Interface Invalid Reports were not reviewed by a supervisor to ensure all exceptions noted on the report had been corrected by the payroll technician.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
8	Controls provide reasonable assurance that current- or prior-period adjustments to employee's pay, including employee debt, tax deduction or deductions not taken, are reported, reconciled and approved.	Policies and procedures are documented to describe that management ensures current- or prior-period adjustments to employee's pay, including employee debt, tax deduction or deductions not taken, are reported, reconciled and approved.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the processing of current or prior-period adjustments to employee's pay, including employee debt, tax deduction or deductions not taken, existed and were documented.	**No relevant exceptions noted.**
		The detailed "592" payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inspected a sample of 20 (to include all pay periods during the 9 month audit period) "592" reconciliations for each database and inquired with appropriate personnel to confirm: • The detailed payroll reconciliation showed pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances were reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; • Each "592" reconciliation was approved by management prior to disbursement and; • Reconciling items were investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	**No relevant exceptions noted.**
		OLQs and summary reports such as the Master Employee Add/Change/Delete Report are periodically reviewed by supervisory personnel to determine if the master files remain accurate and pertinent.	Inspected OLQs and Master Employee Add/Change/Delete reports, observed payroll office staff summary report and OLQ review procedures, and inquired with appropriate personnel to confirm that	DFAS Charleston The OLQs and Master Employee Add/Change/Delete reports were not signed off to indicate they were reviewed. However, as a mitigating circumstance, we observed that the

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			master files were periodically reviewed by supervisory personnel.	Payroll Office staff reviewed the summary reports; and the reports were archived indicating that they had been run.
		The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Inquired with appropriate personnel and inspected a haphazard sample of 45 access request forms to confirm the master file is restricted to authorized personnel.	Payroll Office Users Seven of 45 payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, one of 45 payroll office user's SAAR forms selected for testing did not contain a supervisor's signature. Non-Payroll Office Users Four of 45 non-payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, four of the 45 non-payroll office users' SAAR forms could not be located.
		Requests to change the payroll master file data and withholding table are submitted on prenumbered Remedy Tickets; the numerical sequence of the Remedy Tickets is accounted for to ensure that the requested changes are processed timely. Access to source documents is controlled and key source documents require signatures from management.	Inspected a random sample of 45 Remedy Tickets and inquired with appropriate personnel to confirm the requests: • Were prenumbered; • That the sequence was accounted for so that the Remedy Tickets were accounted for timely; • That access to the source documents was restricted, and That key source documents had	DFAS-Denver One out of 45 Remedy Tickets selected was not completed within the required time frame. DFAS-Pensacola Four out of 45 Remedy Tickets were not completed within the required time frame. DFAS-Charleston Two out of 45 Remedy Tickets were not completed within the required time frame.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			required signatures from management.	
9	All application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes.	Policies and procedures are documented to describe that application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the identification and authentication of DCPS users existed and were documented.	**No relevant exceptions noted.**
		On-line access logs are maintained by the System Management Office (SMO), and the logs are reviewed regularly for unauthorized access attempts.	Inspected access logs and emails for unauthorized access attempts and inquired with appropriate personnel to confirm that logs were maintained by the SMO, and the logs were reviewed regularly for unauthorized access attempts.	**No relevant exceptions noted.**
		Each operator is required to have a completed a systems access authorized authorization form before being granted access to the system. The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Inspected a randomly selected sample of 45 user authorization forms and inquired with appropriate personnel to confirm the user on the form was properly authorized and that the access granted on the form matched the access granted within DCPS.	<u>Payroll Office Users:</u> Seven of 45 payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS; and one of 45 payroll office user's SAAR forms selected for testing did not contain a supervisor's signature. <u>Non-Payroll Office Users:</u> Four of 45 non-payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, four of the 45 non-payroll office users' SAAR forms could not be located.
		Departmental managers periodically review listings, such as the Personnel/Payroll Reconciliation and Control of Hours Report, of current	Inspected the Personnel/Payroll Reconciliation and Control of Hours Reports and inquired with appropriate personnel to confirm the reports were	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		employees within their departments and notify the personnel department of necessary changes.	generated and being reviewed by management.	
10	Controls provide reasonable assurance that data transmissions in DCPS from user organizations are authorized, complete, accurate and secure.	Policies and procedures are documented to describe that management ensures data transmissions in DCPS from organizations are authorized, complete, accurate and secure.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the processing of DCPS data transmissions existed and were documented.	**No relevant exceptions noted.**
		Compliance with the payroll disbursement processing schedule is monitored by management.	Inspected pay processing schedules, observed the payroll disbursement process, and inquired with appropriate personnel to confirm the management monitored and reviewed the payroll disbursement processing schedule.	**No relevant exceptions noted.**
		Each operator is required to have a completed systems access authorized authorization form before being granted access to the system. Authorization profiles over users limit what transactions data entry personnel can enter.	Inspected a randomly selected sample of 45 user authorization forms and inquired with appropriate personnel to confirm that each operator was required to have an authorization form before being granted access to the system and that profiles for user's limit what transactions data entry personnel can enter.	Payroll Officer Users: Seven of 45 payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS; and one of 45 payroll office user's SAAR forms selected for testing did not contain a supervisor's signature. Non-Payroll Office Users: Four of 45 non-payroll payroll office users' SAAR forms selected for testing contained an authorization for access on the SAAR form, which did not match access granted within DCPS. In addition, four of the 45 non-payroll office users' SAAR forms could not be located.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Remote terminal connections are secured and are connected via government issued computers.	Observed remote terminal connections and inquired with appropriate personnel to confirm they were secured and are connected via government computers.	DFAS-Charleston Users had access to DCPS from remote locations using Secure Web Access over non-DoD furnished equipment. As a mitigating circumstance, these users were still subject to DCPS user access controls (for example, a user would still have to sign into DCPS with a unique user ID and password).
		Data entry terminals are connected to the system only during specified periods of the day, which corresponds with the business hours of the data entry personnel.	Observed after-hours processes and inquired with appropriate personnel to confirm terminals were not connected after business hours.	**No relevant exceptions noted.**
		User identification (ID) and passwords are required to gain access to the DCPS application.	Observed the DCPS log-in process and inquired with appropriate personnel to confirm that user IDs and passwords were required to gain access to the DCPS application.	**No relevant exceptions noted.**
		On-line access logs are maintained by the SMO, and the logs are reviewed regularly for unauthorized access attempts.	Inspected access logs and emails and inquired with appropriate personnel to confirm that logs were maintained by the SMO and the logs were reviewed regularly for unauthorized access attempts.	**No relevant exceptions noted.**
		Each terminal automatically disconnects from the system when not used after a specified period of time.	Observed system inactivity and Inquired with appropriate personnel to confirm that each terminal automatically disconnected from the system when not used after a specified period of time.	**No relevant exceptions noted.**
		When terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	Observed facility and inquired with appropriate personnel to confirm that when terminals were not in use, terminal rooms were locked, or the terminals were capable of being secured.	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
11	Controls are reasonable to ensure that transmissions from interfacing systems are subjected to the payroll system edits, validations and error-correction procedures.	Policies and procedures are documented to describe that transactions from interfacing systems are subjected to the payroll system edits, validations and error-correction procedures.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the processing of interface files existed and were documented.	**No relevant exceptions noted.**
		A control group is responsible for controlling and monitoring rejected transmissions included on the Personnel Interface Invalid Report.	Inspected a haphazard sample of 45 Personnel Interface Invalid Reports and inquired with appropriate personnel who clear the Personnel Interface Invalid Reports to confirm the reports were used to identify and resolve rejected transmissions.	<u>DFAS-Denver</u> Due to technical difficulties with the document management system used to store the Personnel Interface Invalid Reports, the Personnel Interface Invalid Reports could not be provided prior to March 27, 2005, which represented 18 of the 45 reports selected for testing. Additionally, one of the remaining 27 reports available from March 28, 2005 through June 30, 2005 could not be located, which left the sample of 26 to be reviewed. Annotations on 23 of the 26 Personnel Interface Invalid Reports from March 28, 2005 through June 30, 2005 did not include the corrective actions taken; 18 out of the 26 Personnel Interface Invalid Reports provided were not dated as completed, and 12 of the 26 Personnel Interface Invalid Reports were not initialed as completed. <u>DFAS-Charleston</u> Due to the inability of the system to allow annotation of the Personnel Interface Invalid Reports and payroll office personnel performed an undocumented random review of the reports instead of a documented

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				review all reports, the audit team could not determine that the Personnel Interface Invalid Reports are properly corrected, annotated, and reviewed by supervisors. Therefore, testing of the reports at DFAS Charleston payroll office was not performed. DFAS-Pensacola Ten of the 44 Personnel Interface Invalid Reports were not available for review. The remaining 34 reports that were reviewed did not always have the final resolution of errors annotated in the report. The Personnel Interface Invalid Reports were not reviewed by a supervisor to ensure all exceptions noted on the report had been corrected by the payroll technician.
		The data processing control group has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; reviews output products for general acceptability; and reconciles control information to determine completeness of processing.	Inspected schedules used by the data processing group and inquired with appropriate personnel to confirm they: • Had a schedule by application that showed when outputs needed to be completed, when they needed to be distributed, who the recipients were, and the copies needed; • Reviewed output products for general acceptability, and • Reconciled control information to determine completeness of processing.	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		The system provides an audit trail of all transactions processed, transaction errors, error descriptions, and error correction procedures. Audit trails are reviewed by supervisory personnel and erroneous data are captured, reported, investigated, and corrected.	Inspected audit trails of transactions and inquired with appropriate personnel to confirm that erroneous transactions were reviewed by supervisory personnel, captured, reported, investigated, and corrected.	**No relevant exceptions noted.**
		For interfacing systems, record counts are accumulated and compared to footer control totals to help determine the completeness of interface processing. Out-of-balance conditions are reported, corrected and reentered.	Inspected interface files and inquired with appropriate personnel to confirm that record counts matched control totals in the footer to determine completeness of interface processing and that out-of-balance conditions were reported, corrected and reentered.	**No relevant exceptions noted.**
		Batch transactions without pre-assigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.	Observed batch process monitoring to confirm transactions without pre-assigned serial numbers were automatically assigned a unique sequence number.	**No relevant exceptions noted.**
12	Controls provide reasonable assurance that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency specific guidelines.	Policies and procedures are documented to describe that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency specific guidelines.	Read policies and procedures and inquired with appropriate personnel to confirm that policies and procedures related to the maintenance of personnel payroll records and other sensitive information existed and were documented.	**No relevant exceptions noted.**
		All documents and storage media are stored in physically and environmentally secure containers.	Observed storage processes and inquired with appropriate personnel to confirm documents and storage media were stored properly in environmentally secure containers.	**No relevant exceptions noted.**
		All visitors to the Payroll Office must sign-in and out with the authorized security personnel.	Inspected visitor logs to the payroll office and inquired with appropriate personnel to observe that visitors signed in with the authorized security personnel.	**No relevant exceptions noted.**

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		All terminals and payroll records are located in physically secured locations.	Observed the terminal rooms and inquired with appropriate personnel to confirm that access to the rooms was restricted.	**No relevant exceptions noted.**
		Users dispose of personnel and payroll records in accordance with government-wide and agency-specific guidelines.	Observed destruction bins and inquired with appropriate personnel to confirm that payroll records were disposed of in accordance with Government-wide and agency-specific guidelines.	**No relevant exceptions noted.**

General Computer Control Objectives, Activities, Test Procedures and Results of Testing

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	Enterprise-Wide Security Program Planning			
1	Risks are periodically assessed.	DFAS-Pensacola DoD and DFAS policy both direct an annual Information assurance review. Review appropriate generated documentation to ensure that these processes are accomplished.	DFAS-Pensacola Inquired with security personnel regarding the frequency of the risk assessment process. Inspected the latest Risk Assessment documented in the SSAA to confirm that risks were periodically assessed.	**No relevant exceptions noted**
2	A security plan is documented, approved and kept current.	DFAS-Pensacola DoD and DFAS policy both direct an annual Information assurance review. Review appropriate generated documentation to ensure that these processes are accomplished.	DFAS-Pensacola Inspected the DCPS SSAA to confirm it has been documented, kept current and appropriately approved by management. Inspected the DCPS Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each had been updated.	**No relevant exceptions noted**
3				**Control objective left intentionally blank**
4	Owners and users are aware of security policies.	DISA-Mechanicsburg Ongoing security awareness curriculum that include: New Employee Security Briefing; Annual Security Briefing; Information Assurance (IA) Awareness Training; Courier Briefings; SF 312 Non-Disclosure Briefing; Antiterrorism Force Protection Briefings; System Administrator (SA) Training, and a Security Page on Command Intranet site.	DISA-Mechanicsburg Inspected the Security Awareness Training materials to confirm they are documented. Selected a haphazard sample of 45 employees and inspected their training files to confirm the completion of the necessary security training and a signoff. Inspected the training sign-in sheets to	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		DFAS-Pensacola Ongoing security awareness programs that include initial training and periodic refresher training.	confirm that employees attended annual training. Inspected documentation showing that management had active security awareness programs in place that proactively emphasized the security policies to data owners and users. DFAS-Pensacola Inspected the Security Awareness Training materials to confirm they were documented. Selected a haphazard sample of employees and inspected their training files to confirm the completion of the necessary security training and a signoff. Inspected the training database to confirm that employees attended annual training. Inspected documentation that management had active security awareness programs in place that proactively emphasized the security policies to data owners and users.	
5	An incident response capability has been implemented.	DISA-Mechanicsburg DISA Policy Letter 05-04 "Computer Security Incident Handling and Reporting" May 4, 2005, has been implemented.	DISA-Mechanicsburg Inspected the incident plan detailed in the SSAA to confirm it was documented. Selected a haphazard sample of incidents and observed the incidents were addressed based on the incident response plan.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
6	Hiring, transfer, termination, and performance policies address security.	DISA-Mechanicsburg Personnel and Industrial Security Program(s) implemented in accordance with DoD 5200.2-R, DoD Directive (DoDD) 8500.1, DoDI 8500.2, and the Computing Services Security Handbook.	DISA-Mechanicsburg Inspected the hiring, transfer, termination and performance policies to confirm they were documented and addressed security requirements. Inquired with security personnel to confirm that debriefs were conducted when employees were terminated and that a DISA Form 70 was used to note the collection of DISA property. Observed that a checkout form was sent to the System Administrator to document that system access had been removed for a terminated employee.	**No relevant exceptions noted**
7	A training program is implemented to provide assurance that employees have adequate training and expertise.	DISA-Mechanicsburg A robust Security Awareness curriculum that includes: New Employee Security Briefing; Annual Security Briefing; information assurance Awareness Training; Courier Briefings; SF 312 Non-Disclosure Briefing; Antiterrorism Force Protection Briefings; and SA Certification/Training has been implemented. DFAS-Pensacola An ongoing security awareness programs that include initial training and periodic refresher training is implemented.	DISA-Mechanicsburg Inquired with the security personnel to confirm that a training program was established. Inspected documentation to confirm the existence of a training program. Inspected training materials to confirm they provided personnel with adequate training. Selected a haphazard sample of 45 employees who had access to DCPS and inspected their training records to confirm specific job function training was occurring. DFAS-Pensacola Inquired with the Information Security Officer (ISO) to confirm that a training program was established.	There was no structured functional training program established at DISA-Mechanicsburg for all DCPS personnel. In addition, there was no process in place to independently verify users completed training and submitted completion statements. However, DISA-Mechanicsburg did have a process for users to obtain training.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		Additionally the DCPS SSAA includes an Appendix J, System Rules of Behavior, which describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.	Inspected documentation to confirm the existence of a training program. Inspected training materials to confirm they provided personnel with adequate training and expertise. Selected a haphazard sample of 45 employees who had access to DCPS and inspected their training records to confirm specific job function training was occurring.	
8	Management periodically assesses the appropriateness of security policies and compliance with them.	DISA-Mechanicsburg The Director's Policy Letters (DPLs) and Standard Operating Procedures (SOP) are reviewed and updated. SRR are conducted at least every three years.	DISA-Mechanicsburg Inquired with the Security Officer to confirm management assessed the appropriateness of the security policies and compliance with them. Inspected the DCPS Security Requirements and Information Systems Security Policy Certification Test and Evaluation Procedures to confirm that an annual IA review was conducted and that comprehensive vulnerability management was in place.	**No relevant exceptions noted**
9	Management ensures that corrective actions are effectively implemented.	DISA-Mechanicsburg The Vulnerability Management System (VMS) is used to track findings from the SRR process. DECC MECH management is responsible for tracking and closing all findings that resulted from the SRR process.	DISA-Mechanicsburg Observed the SRR process to confirm that corrective actions were effectively implemented for identified SRR findings. Selected a haphazard sample of SRRs and inspected the VMS reports to confirm findings identified by the SRR process were addressed. Inspected prior audit reports or reviews to confirm findings and recommendations presented were	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		DFAS-Pensacola Management tracks the observations of prior audit reports and confirms that observations are corrected in a timely manner.	addressed. DFAS-Pensacola Inspected prior audit reports or reviews to confirm findings and recommendations presented were addressed.	
10	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.	DISA-Mechanicsburg Vulnerabilities are tracked in the VMS database. Prior to connection to the network, the SA must run a VS08 report detailing Information Assurance Vulnerability Management (IAVM) notices for the asset's operating system. All IAVM notices must be mitigated and applicable patches loaded prior to connecting the asset to the network. Once all checklists have been applied from the STIG and the vulnerability alerts have been installed, a SRR and an ISS scan will be conducted of the operating system. Security assessments that require a scan will use the Internet Security Scanner (ISS) and the FSO Full Scan Policy. The scan will be conducted using a direct connection from the system running ISS to the system being assessed or the site is authorized to connect the asset to an isolated network during the ISS scan. Each site will place their self-assessment in the Security Readiness Review Database (SRRDB). If the systems have a database, web server, or any other software that has a STIG, they must go through a FSO SRR and the results put in the self-assessment of the SRR database.	DISA-Mechanicsburg Inspected the vulnerability management policy and documentation to confirm that the process included systematic identification and mitigation of software and hardware vulnerabilities. Inspected the most recent vulnerability assessment to confirm that vulnerabilities were being identified, and resolved after identification. Inspected the VMS reports for the audit period to confirm vulnerabilities were tracked and resolved in a timely manner.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
11	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	DFAS-Pensacola All changes made at are captured in the Change Management Information System (CMIS). Information included in each change record is the requested time and date of implementation, the action to occur, and justification of the action.	DFAS-Pensacola Inquired with DCPS management to confirm that management assessed whether changes complied with Information Assurance requirements and changes impacted accreditation before moving the changes into the production environment. Observed outputs of CMIS to confirm that the information included in each change record included the requested time and date of implementation, the action to occur, and justification of the action.	**No relevant exceptions noted**
12	A DoD reference document constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled Information Technology (IT) products.	DISA-Mechanicsburg DISA has developed and requires compliance with the STIGs appropriate to the operating system, application or hardware.	DISA-Mechanicsburg Inspected the DISA STIG to confirm that they constituted the primary source configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled products.	**No relevant exceptions noted**
	Access Controls			
13	Owners have classified resources and related criteria have been established.	DFAS-Pensacola Management has classified DCPS according to appropriate MAC level standards.	DFAS-Pensacola Inspected the DCPS SSAA and inquired with data owners to confirm that a MAC level was assigned to DCPS.	**No relevant exceptions noted**
14	Resource owners have identified authorized users and their access authorized.	DFAS-Pensacola The SAAR DD-2875 form is used to identify authorized users and control their access.	DFAS-Pensacola Selected a haphazard sample of TSO users from the TSO user list and inspected their user access request forms for existence and approval of management. Observed the DCPS application to confirm that users possessed a valid User ID and password to gain access to the system.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Inquired with security managers to confirm that supporting documentation was provided to them. Reviewed supporting documentation to confirm that inappropriate access was removed in a timely manner. Inspected a haphazard sample of 45 profile changes and activity logs to confirm that management reviewed the changes and logs. Observed the entire population of ten terminated or transferred employees during the audit period to confirm that their system access was promptly terminated within the system.	
15	Emergency and temporary access authorization is controlled.	DISA-Mechanicsburg Emergency and temporary access authorization are controlled in accordance with DoD 5200.1-R; DoD 5200.2-R; DoDD 8500.1; DoDI 8500.2, and Computing Services Security Handbook.	DISA-Mechanicsburg Inspected the emergency and temporary access policy to confirm it was documented. Selected a random sample of 45 days of emergency and temporary access requests and: • Confirmed that the authorization was approved and that access was closed in a timely manner. • Confirmed that the emergency and temporary access list was periodically reviewed. • Confirmed that all temporary access authorizations were established for least privileged need-to-know access.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
16	Owners determine disposition and sharing of data.	DFAS-Pensacola Documented policies and procedures are in the SSAA that govern the sharing of data.	DFAS-Pensacola Inspected documents authorizing file sharing and file sharing agreements to confirm the owners approved the sharing of data. Inspected the DCPS SSAA to confirm that a MAC level was assigned to DCPS. Inquired with key personnel to confirm that a MOA or a MOU was documented for all interfaces into DCPS.	Forty-three of 148 DCPS interfaces did not have a documented MOA or MOU
17	Adequate physical security controls have been implemented that are commensurate with the risks of physical damage or access.	DISA-Mechanicsburg All DISA facilities at DECC ME are locked at all times. Access is restricted using proximity cards, with PIN technology, which are controlled and issued by the Security Manager. The Naval Inventory Control Point conducts periodic, unannounced penetration testing to confirm that physical security is adequate. DECC MECH SSAA requires the performance of physical security inspections by the Security Office.	DISA-Mechanicsburg Observed that physical safeguards were in place. Observed that facility penetration testing processes were in place.	**No relevant exceptions noted**
18	Visitors are controlled.	DISA-Mechanicsburg Visitor's are controlled in accordance with DoD 5200.2-R; 5200.1-R and the Computing Services Security Handbook. Utilize access control database; proxy/pin technology; vetted badge exchange; Access Control Monitor Personnel; visitors log, Visit authorization Requests.	DISA-Mechanicsburg Inspected the visitor policy, procedures, and logs to confirm they were documented. Observed the visitor check-in and check-out process to confirm visitors were logged.	The visitors log used by the DFAS TSO facility was not fully completed for each visitor. However, all visitors had visitor badges that required them to enter the facility through only one guarded entrance.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		DFAS-Pensacola All visitors must sign-in and out with the guard on duty. The DCPS SSAA requires all non-cleared personnel to be escorted at all times while inside the building.	Inquired with physical security personnel and observed that visitor access to DoD information was determined by both its classification and user need-to-know. DFAS-Pensacola Inspected the visitor policy and procedures to confirm it was documented. Observed the visitor check-in and check-out process to confirm all visitors were logged. Inquired with physical security personnel and observed that visitor access to DoD information was determined by both its classification and user need-to-know.	
19	Adequate logical access controls have been implemented at the application layer.	User IDs and passwords are configured according to DISA standards.	DFAS-Pensacola Observed that each TSO user account was assigned a security profile that restricted access. Selected a haphazard sample of 45 TSO users from the TSO user list and inspected their user access request forms for existence and approval of management. Observed the DCPS application to confirm that TSO users possessed a valid User ID and password to gain access to the system. Inquired with security personnel and observed supporting documentation to confirm that inappropriate access was	The current version of Access Control Facility 2 (ACF2) does not allow for password character complexity as required by DoDI 8500.2. However, access to DCPS was still subject to password controls that included periodic changing and minimum character lengths.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			removed in a timely manner. Confirm that password parameters were in compliance with DoD Instruction 8500.2 password requirements. Inspected documentation for a haphazard sample of 45 terminated employees to confirm that system access was promptly terminated.	
20	Passwords, tokens, or other devices are used to identify and authenticate users.	DFAS-Pensacola Multiple layers of access controls are used including; Common Access Card (CAC) and personal identification number, DCPS userid and password, and a RSA SecurID for Database Administration, Configuration Management, Security, and Tech Support.	DFAS-Pensacola Observed the DCPS application to confirm that users needed a valid User ID and Password to gain access to the system. Inspected system parameters to confirm that the system required a User ID and Password.	**No relevant exceptions noted**
21	Access paths are identified as part of a risk analysis and documented in an access path diagram.	DISA-Mechanicsburg Access paths are identified as part of the Mechanicsburg Enclave SSAA and documented in the network diagram within the SSAA. Firewalls and routers are used to restrict access within the network.	DISA-Mechanicsburg Inquired with network support personnel that user management controls, firewalls, intrusion detection systems (IDS), and authentications were all used to control network access. Inspected the network diagrams for DISA-Mechanicsburg to confirm that access paths were documented and monitored by intrusion detection systems.	The firewalls supporting the access path to DCPS were no longer supported by the vendor and, therefore, were not configured with rules. To compensate for the lack of firewall rules, the routers supporting this access path were configured to deny all requests except for items included on their access control lists.
22	Access is restricted to data files and software programs.	DISA-Mechanicsburg The DISA System Support Office (SSO), a unit independent of DECC operations, is responsible for maintaining the system libraries. Access to system libraries is restricted	DISA-Mechanicsburg Inspected ACF2 user profiles for the DCPS system to confirm that administrator level access restrictions were established around the data files and software programs.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		to authorized individuals	Inspected the access logs and inquired with security personnel to confirm that the access logs were reviewed for inappropriate access and that system libraries were managed and maintained to protect privileged programs.	
23	Access settings have been implemented in accordance with the access authorizations established by the resource owners.	DISA-Mechanicsburg Access settings have been implemented in accordance with the access authorizations established by signature authority of resource owner on Form DD2875 and in accordance with DoDD 8500.1; DoDI 8500.2 and STIGs. DFAS-Pensacola The Technical Support Office assigns security profiles to each userid based on need to know as demonstrated by an approved Form DD2875, request for system access. TSOPE Database Administrator also assigns security profiles to development users through the Integrated Database management System (IDMS) which restricts access to program libraries and databases.	DISA-Mechanicsburg Inspected a haphazard sample of SAAR Form DD2875s to confirm that each form detailed the system support user's justification for access, security clearance level, and that each Form DD2875 was properly approved. DFAS-Pensacola Inspected a haphazard sample of SAAR Form DD2875s to confirm that each form detailed the TSO user's justification for access, security clearance level, and that each Form DD2875 was properly approved.	Access justification was not documented on the Form DD2875 for four of 45 DISA-Mechanicsburg personnel. One of 45 users had access to the DCPS production environment that was not authorized on their Form DD2875.
24	Telecommunications controls are properly implemented in accordance with authorizations that have been granted.	DISA-Mechanicsburg Remote access to the Internet is regulated by positive technical controls such as firewalls, routers, and proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means. There is a remote dial-in router provided for Systems Administrators	DISA-Mechanicsburg Inspected the telecommunications policy to confirm that is was documented. Observed the existence telecommunication monitoring controls. Obtained firewall rules to confirm they were documented.	The firewalls supporting the access path to DCPS were no longer supported by the vendor and, therefore, were not configured with rules. To compensate for this lack of firewall rules, the routers supporting this access path were configured to deny all requests except for items included on their access control list.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		which requires Secure Shell restrictions. Enterprise Security Manager is installed on some of these systems.		
25	Procedures are in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use.	DISA-Mechanicsburg All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released, and sign off is required to certify the destruction of such media.	DISA-Mechanicsburg Inspected the Disposition of Unclassified DoD Computer Hard Drives policy to confirm it was documented. Observed the access controls to the media while it was waiting to be cleared or destroyed. Observed the procedures in place to clear or destroy equipment and media.	**No relevant exceptions noted**
26	Audit trails are maintained at the application layer, operating system (OS), and database layer.	DISA-Mechanicsburg and DFAS-Pensacola A security audit trail is implemented for each system that documents the identity of each person/device having access to a system, the time of that access, user activity, and any actions which attempt to change security levels or privileges established for the user.	DISA-Mechanicsburg Inquired with security personnel to confirm that audit trails were implemented at the application and operating system levels. Inspected the audit log to confirm system information was logged. Inquired with security personnel and observed that audit trails were maintained. DFAS-Pensacola Inquired with security personnel to confirm that audit trails were implemented at the application and operating system levels. Inspected the audit log to confirm system information was logged. Inquired with security personnel and	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			observed that audit trails were maintained.	
27	The contents of audit trails are protected against unauthorized access, modification or deletion.	DISA-Mechanicsburg Contents of audit trails are protected in accordance with STIGs and the DISA Computing Services Security Handbook. User's authorization for access to various systems is identified in each individual's new user agreement (completed when account is created). DFAS-Pensacola Adheres to DITSCAP requirements for system access and content, retention and protection of audit trails. The most recent testing of compliance with DITSCAP guidance is contained in the DCPS SSAA, Appendices H and P.	DISA-Mechanicsburg Confirmed that policies were documented to limit access to audit trails. Observed access to the audit logs to confirm that activities that might modify, bypass, or negate safeguards controlled by the system and the audit trails were protected against unauthorized access, modification, or deletion. Observed that only selected/limited number of individuals such as the ISSO and Information Assurance Manager had access to the audit trails. DFAS-Pensacola Confirmed that policies were documented to limit access to audit trails. Observed access to the audit logs to confirm that activities that might modify, bypass, or negate safeguards controlled by the system and the audit trails were protected against unauthorized access, modification, or deletion. Observed that only selected/limited number of individuals such as the ISSO and Information Assurance Manager had access to the audit trails.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
28	Tools are available for the review of audit records and for report generation from audit records.	DISA-Mechanicsburg Tools are available for review through System Management Facility, DISPATCH and ACF2 report facility.	DISA-Mechanicsburg Observed the audit tools to confirm they existed. Observed that reports were being generated and that they were reviewed by system security personnel.	**No relevant exceptions noted**
29	Actual or attempted unauthorized, unusual, or sensitive network access is monitored and suspicious or irregular access activity is investigated and appropriate action taken.	DISA-Mechanicsburg ACF2 is maintained at both DECC MECH and the various payroll offices by a series of security administrators with differing roles (administration, user accounts etc.) The logs are centrally reviewed at DECC MECH. Multiple unsuccessful login attempts result in the account being locked. If the account is unused for a specified period then the account is deactivated.	DISA-Mechanicsburg Inspected copies of the policies and procedures relating to access controls to confirm they were documented. Inquired with the System Security Administrator to confirm that system access such as unauthorized, unusual, or sensitive access is monitored. Inquired with the SA to confirm that suspicious or irregular access activity was investigated and responses were taken. Inspected audit log reviews and incident reports to confirm that investigations and actions were taking place.	**No relevant exceptions noted**
30	The acquisition, development, and/or use of mobile code to be deployed in DoD systems meet current guidelines, standards and regulations.	DISA-Mechanicsburg Use of mobile code is only permitted following a risk assessment, categorization of the mobile code, and counter measures have been implemented. A waiver has been obtained from the responsible Chief Information Officers office.	DISA-Mechanicsburg Inspected the DoD systems guidelines, standards, and regulations concerning mobile codes to confirm they were documented. Inquired with the System Administrator to confirm that the acquisition, development, and/or use of mobile code to be deployed in DoD systems met current guidelines, standards and regulations.	Software that supports mobile code was found on the DCPS production Logical Partition (LPAR). ACF2 was configured to prevent non authorized code from running on the DCPS LPAR.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Inspected a list of software on the DCPS production environment for software that supported mobile codes.	
31	All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.	DISA-Mechanicsburg Anti-virus software is installed on personal computers, laptops, and systems under DECC MECH control.	DISA-Mechanicsburg Observed that servers, workstations and mobile computing devices implemented virus protection that allows the capability of automatic updates.	**No relevant exceptions noted**
32	All Virtual Private Network (VPN) traffic is visible to network IDS.	DISA-Mechanicsburg ISS Real Secure is installed at various points that give visibility into the network traffic ingressing and egressing the enclave.	DISA-Mechanicsburg Inquired with SAs to confirm that all VPN traffic is visible to network IDS. Inspected system network diagram and inquired with the SA to confirm that VPN traffic is included on the diagram.	**No relevant exceptions noted**
33	At a minimum, medium-robustness Commercial Off-the-Shelf (COTS) IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.	DISA-Mechanicsburg Appropriate IA products are implemented to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.	DISA-Mechanicsburg Inquired with security personnel to confirm that at a minimum, medium-robustness COTS IA and IA-enabled products were used to protect sensitive information when the information transits public networks or the system handling the information was accessible by individuals who were not authorized to access the information on the system for each of the DCPS locations. Observed the use of access control software to confirm access to data was controlled.	**No relevant exceptions noted**
34	Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation.	DISA-Mechanicsburg Work stations are locked systematically after a period of inactivity in accordance with DoDI 8500.2. A password is required to unlock the workstation.	DISA-Mechanicsburg Observed a haphazard sample of workstations to confirm screen-lock functionality was applied.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		DFAS-Pensacola The Desktop Management Initiative (DMI) (not associated with TSOPE) controls the configuration of all DFAS computers including the operating system and the application of screen-lock functionality.	DFAS-Pensacola Observed a haphazard sample of workstations to confirm screen-lock functionality was applied.	
35	Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems.	DISA-Mechanicsburg Use of Instant Messaging applications is not permitted and network personnel monitor common Firewall and system ports to identify and eliminate the use of instant messaging applications. DFAS-Pensacola DMI controls the configuration of computers and instant messaging program are not authorized. TSOPE monitors application usage through an automated software auditing application that runs regularly when users logon to their workstation. Instant messaging programs are identified as part of that auditing process.	DISA-Mechanicsburg Inquired with security personnel to confirm that the use of instant messaging is against policy. Inspected firewall/router access control lists (ACL) rules to confirm instant messaging was blocked. DFAS-Pensacola Inquired with security personnel to confirm that the use of instant messaging was against policy. Inquired with security personnel to confirm firewall rules were configured to block instant messaging. Inspected workstations to confirm that instant messaging software was not loaded and users did not have administrative rights to computer.	**No relevant exceptions noted**
36	For Automated Information System (AIS) applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and	DISA-Mechanicsburg and DFAS-Pensacola All interconnections of DoD information systems are to be managed continuously to minimize risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected	DISA-Mechanicsburg Inspected the site SSAA to confirm the DCPS enclave was identified and documented. DFAS-Pensacola Inspected the Service Level Agreement between DISA and DFAS to confirm	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	requirements.	systems	evidence of deployment planning and coordination, and the exchange of connection rules and requirements.	
37	Group authenticators for application or network access may be used only in conjunction with an individual authenticator.	DISA-Mechanicsburg and DFAS-Pensacola Group authenticators are not used for DCPS or network access. Upon initial system login, a user's actions are tracked based on their unique user account.	DISA-Mechanicsburg Inquired with system security personnel to confirm group authenticators for application, network or operating system were used. If so, inquired to understand the reason behind the usage of group authenticators. (In many cases it was a system limitation) If so, inquired if users were authenticated individually prior to the use of a group authenticator. DFAS-Pensacola Confirmed through inquiry if group authenticators for application and network were used. If so, inquired to understand the reason behind the usage of group authenticators. (In many cases it was a system limitation) If so, inquired if users were authenticated individually prior to the use of a group authenticator.	The DFAS-Pensacola personnel who work in the DCPS operations room used group authentication to facilitate the operations and maintenance of various payroll databases.
38	To help prevent inadvertent disclosure of controlled information, all contractors and foreign nationals are identified by e-mail addresses and display names.	DISA-Mechanicsburg Exchange Server Administration includes the specific configuration of email addresses and display names for contractors and foreign nationals.	DISA-Mechanicsburg Obtained and inspected a listing of email addresses for DCPS contractors and foreign nationals to confirm their display names identified them as contractors or foreign nationals.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
39	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using National Institute of Standards and Technology (NIST)-certified cryptography.	DISA-Mechanicsburg Encryption data streams are in the process of conforming to the Federal Information Processing Standards-140-2 standard.	DISA-Mechanicsburg Inquired with security personnel to confirm DCPS data was transmitted through a commercial or wireless network and NIST cryptography was used to protect information when the information transmitted over commercial or wireless networks.	Sensitive but unclassified personnel and payroll data transmitted within DoD internal networks was not encrypted; however, DCPS traffic transmitted on non-DoD networks was encrypted.
40	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules.	DISA-Mechanicsburg The SSAA requires that access to all DoD information systems shall be based on a demonstrated need-to-know and granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R.	DISA-Mechanicsburg Inspected the user list from the Discretionary Access Control (DAC) of all individuals who had direct access to the system software to confirm their access was limited to a need-to-know basis.	**No relevant exceptions noted**
41	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted.	DISA-Mechanicsburg Performs monthly vulnerabilities scans. DCPS and its hardware are reviewed by a FSO SRR.	DISA-Mechanicsburg Inquired with security personnel that conformance testing was performed that included periodic, unannounced, in-depth monitoring and provided for specific penetration testing to confirm compliance with all vulnerability mitigation procedures were planned, scheduled, and conducted. Inspected documentation produced from conformance testing to confirm such testing was performed.	**No relevant exceptions noted**
42	All users are warned that they are entering a Government information system.	DISA-Mechanicsburg All DISA networks and platforms present a message to users upon logon, which warns them that they are entering a Government information system, and	DISA-Mechanicsburg Observed that the DCPS LPAR system parameters were set to display a DoD warning banner for initial end user connections.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.		
43	Information and DoD information systems that store, process, transmit, or display data in any form or format that is not approved for public release comply with requirements in policy and guidance documents and information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography.	DISA-Mechanicsburg Information on DoD systems that store, process, transit, or display data in any format that is not approved for public release complies with DoD policy. Access to all DoD information systems is based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access and IT position designations and requirements	DISA-Mechanicsburg Observed the DECC MECH data center, including onsite tape storage areas, to confirm that labels indicating classification level were affixed to all computers and storage devices. Inquired with security personnel to confirm that information in transit through the network was encrypted. Inquired with security personnel to confirm the usage of a network monitoring tool.	Sensitive but unclassified personnel and payroll data transmitted within DoD internal networks was not encrypted; however, DCPS traffic transmitted on non-DoD networks was encrypted.
44	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a DMZ and boundary defense mechanisms to include firewalls and network IDS are deployed at the enclave boundary.	DISA-Mechanicsburg Perimeter firewalls, routers, and intrusion detection systems are implemented. DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called DMZ, or through systems that are isolated from all other DoD information systems through physical means.	DISA-Mechanicsburg Inspected the system architecture to confirm that connections between DoD enclaves and the Internet were configured with a DMZ, and boundary defense mechanisms included firewalls and network IDS were deployed at the enclave boundary. Inspected system network diagram and inquired with the SA to confirm that a DMZ and defense mechanisms were employed. Observed the existence of firewalls and IDSs.	The firewalls supporting the access path to DCPS were no longer supported by the vendor and, therefore, were not configured with rules. To compensate for this lack of firewall rules, the routers supporting this access path were configured to deny all requests except for items included on their access control list.
45	Devices that display or output classified or sensitive information in human-readable form (monitors and printers) are	DISA-Mechanicsburg Devices that display or output classified information are labeled to indicate whether classified information	DISA-Mechanicsburg Observed that displays and printers used for sensitive information were positioned to deter unauthorized	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	positioned to deter unauthorized individuals from reading the information.	can be displayed. All devices are located in Approved Open Collateral Storage Areas. Access to these areas is controlled. DFAS-Pensacola Access to systems containing sensitive information display warning banners upon login to warn authorized users; unauthorized users are denied while attempting to login to the system. Individuals who print sensitive information in human-readable form have localized printers. Each user outputting sensitive data in human readable form is accountable for the security in handling of that information.	individuals from reading the information. DFAS-Pensacola Observed that displays and printers used for sensitive information were positioned to deter unauthorized individuals from reading the information.	
46				**Control objective left intentionally blank**
47	DoD information systems comply with DoD ports, protocols, and services guidance.	DISA-Mechanicsburg DCPS-related ports, protocols, and services are configured according to DoD guidance.	DISA-Mechanicsburg Confirmed though inquiry with DISA personnel and observed the DCPS routers ACL that DCPS complied with DoD ports, protocols, and services guidance, including all ports, protocols, and services. Observed that ports, protocols, and services were identified and registered. Inspected the latest SRR report and remediation of findings of DCPS to confirm DISA was monitoring compliance with the DISA STIG.	**No relevant exceptions noted**
48	Binary or machine executable public domain software products and other software products with	DISA-Mechanicsburg Public domain software products, and other software products with limited or	DISA-Mechanicsburg Inspected a listing of software products installed on the DCPS mainframe to	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	limited or no warranty are not used in DoD information systems.	no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible Designated Approving Authority.	confirm DCPS does not have binary or machine executable public domain software and other software products with limited or no warranty installed on DCPS.	
	Application Software Development and Change Control			
49	A system development life cycle methodology (SDLC) has been implemented and documented.	There is a defined configuration management (CM) process in place at DFAS-Pensacola. The process is documented in the SSAA under Appendix S – Change Management Plan. Included in the plan are: • Formally documented CM roles, responsibilities and procedures including management of IA information and documentation; • The detailed role of the CCB including its roles for reviewing and approving changes; • The testing process that all changes must go through, including the migration of the change from the development region to the testing region, and the testing region to production;	<u>DFAS-Pensacola</u> Inspected the Configuration Management Plan to confirm that it was documented.	**No relevant exceptions noted**
50	Authorizations for software modifications are documented and maintained. This should also include emergency changes	<u>DFAS-Pensacola</u> A Configuration Management Plan is implemented for software modifications; contained in the DFAS TSO Business Process Handbook. All modifications must go through the System Change Request (SCR) process	<u>DFAS-Pensacola</u> Inspected the full population of modifications occurring during the audit period to confirm they were supported by an approved SCR or Preliminary Technical Review authorized by the Program Manager and/or Software Director, and supported by a Release Authorization	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		and receive proper approvals prior to implementation, including emergency changes made during business hours. Emergency changes which arise during non-business hours may be implemented prior to SCR approval; however, the change is run through the SCR process at the start of the next business day.	Report.	
51	Use of public domain and personal software is restricted.	DFAS-Pensacola Does not allow any use of public domain and/or personal software. DCPS is on the mainframe; all utilities needed are on the mainframe (which is DISA-driven).	DFAS-Pensacola Inspected public domain and personal software policy to confirm that personal software restrictions were documented. Inspected a listing of installed software to confirm public and personal software was not installed on the DCPS system.	**No relevant exceptions noted**
52	Changes are controlled as programs progress through testing to final approval to ensure completeness, authorization, software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	DFAS-Pensacola Testing of changes follows the approved process outlined in the DFAS TSO Business Process Handbook prior to implementation. A Testing Deficiency Report is issued for SCRs with negative test results and the TDR is routed to the appropriate individuals. If necessary, an amendment is issued and processes through same approval process as an SCR.	DFAS-Pensacola Inspected the entire population of 50 modifications to the application software to confirm they were supported by appropriate test and migration documentation such as System Test Plan, Detailed system specifications; and Unit, System and Acceptance testing results. Inquired with DCPS security personnel and confirmed they reviewed security-related changes included in DCPS Releases. Observed release notes for all major DCPS production releases that occurred during the audit period to confirm release information was documented and communicated.	The appropriate test documentation was provided for the three major quarterly releases. However, TSO was unable to collect and distribute the appropriate test documentation for the remaining 47 interim releases during our audit fieldwork. Management indicated they could not provide this documentation due to the workload of TSO and the time constraints of this audit.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
53	Distribution and implementation of new or revised software is controlled.	DFAS-Pensacola Release Management staff are responsible for distribution or implementation of new or revised software.	DFAS-Pensacola Inspected the full population of 50 modifications and confirmed that changes were supported by a Release Authorization Report.	**No relevant exceptions noted**
54	Programs are labeled and inventoried.	DFAS-Pensacola Release Management staff is responsible for ensuring that all programs are labeled and inventoried within the appropriate library.	DFAS-Pensacola Inspected the full population of 50 modifications to confirm changes were labeled, assigned an ID, and inventoried.	**No relevant exceptions noted**
55	Access to program libraries is restricted to appropriate personnel to ensure that the movement of programs and data among libraries is controlled.	DFAS-Pensacola The System Administrator manages access rights to the program libraries and databases through ACF2. The Database Administrator grants access to the appropriate development/production environments through IDMS. IDMS controls versioning in both the development and production environments.	DFAS-Pensacola Observed the procedures performed by the DCPS Librarian to confirm development and production libraries were controlled. Inspected the access control lists for the Production and Development libraries (directories) to confirm that only authorized personnel had access.	**No relevant exceptions noted**
56	Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.	DFAS-Pensacola The service level agreement between DFAS and DECC MECH explicitly states IA roles and responsibilities for both customer and service provider, “Business processes supported by private sector information systems and outsourced information technologies shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451. Data shall be collected to support reporting and IA management activities across the investment life cycle”	DFAS-Pensacola Inspected the service level agreement contract agreement to confirm it addressed Government, service provider and end-user IA role and responsibilities.	**No relevant exceptions noted**
57	The acquisition of all IA- and IA-enabled Government Off-the-Shelf (GOTS) IT products is	DFAS-Pensacola The SSO is responsible for reviewing and approving all COTS IT products.	DFAS-Pensacola Inquired with security personnel to confirm they verified NSA evaluation	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes.		or conducted an evaluation in accordance with NSA approval for IA related products.	
	System Software Controls			
58				**Control objective left intentionally blank**
59	Policies and techniques have been implemented for using and monitoring use of system utilities.	DISA-Mechanicsburg Access to the system software is administered based on roles.	DISA-Mechanicsburg Inquired with security personnel to confirm root and other privileged access were restricted. Obtained the list of individuals with root and or privileged access and inquired with management that root and privileged access was appropriate and that the use of these accounts was logged. Inspected the policies and procedures for the monitoring of systems software and confirmed they exist and were current. Inspected a sample of the audit logs from the DCPS system to confirm that key personnel review the logs on a regular basis and that any issues noted were documented and researched.	**No relevant exceptions noted**
60	System software changes are authorized, tested, and approved and documented before implementation.	DISA-Mechanicsburg Procedures addressing the testing of patches, upgrades, and new AIS applications are documented. All changes made at DECC MECH are captured in the Change Management System (Change Management 2000). Information included in each change record is the requested time and date of implementation, the action to occur,	DISA-Mechanicsburg Obtained and inspected the change management policies and procedures for systems software to confirm they exist and were current. Obtained a list of all DCPS system software modifications from October 1, 2004 through June 30, 2005 and selected a haphazard sample of	System software change testing results were not required to be documented and maintained. Therefore the audit team was unable to verify that changes were tested prior to movement into the production environment. The charter for the local CCB

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		and justification of the action. All changes to information systems at DECC MECH are brought before at least one of two CCBs. DISA headquarters has Executive software CCB which is responsible for reviewing all major system changes such as new versions, new software, and the removal of software. There is also a local CCB at DECC MECH that meets on a weekly basis. The local CCB is responsible for reviewing all operating system upgrades and fixes. The local CCB is also responsible for alerting the customer to the change and obtaining the customer approval before proceeding. Also, the local CCB is responsible for maintaining the change control records. The DISA Executive Software CCB consists of representative of DISA management as well as all the DISA-DECCs. The DECC MECH local CCB consists of all department heads and the Information Assurance Manager.	45 system software modifications. For each modification selected, obtained the change request document and confirmed that it was approved by key personnel prior to implementation. Confirmed that each modification was tested and the test results were approved prior to the modification being implemented. Confirmed the modification was documented by inspecting the SCR, System Test Plan; Detailed System Specifications; and Unit, System and Acceptance testing results. Observed that there was a charter in place for the CCB.	was not approved.
61	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files.	DISA-Mechanicsburg Implemented COTS software that scans incoming and outgoing files to insure the integrity of those files.	DISA-Mechanicsburg Confirmed through inquiry that a controlled interface was used for interconnections among the DoD information systems that were connected to DCPS. Observed the existence of ACL, IDS, firewalls, encryption, and network monitoring. Confirmed through corroborative	The firewalls supporting the access path to DCPS were no longer supported by the vendor and therefore were not configured with rules. To compensate for this lack of firewall rules, the routers supporting this access path were configured to deny all requests except for items included on their access control list.

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			inquiry that interface inputs were automatically validated by the system for missing information, format, consistency and reasonableness. Observed system batch files of interface inputs for control totals and line counts.	
	Segregation of Duties			
62	Incompatible duties have been identified and policies implemented to segregate these duties.	<u>DFAS-Pensacola</u> Developed distinct system support functions to ensure there is adequate segregation of duties.	<u>DFAS-Pensacola</u> Inspected the organizational chart and the job descriptions for the positions at DFAS-Pensacola in relation to DCPS and confirmed that there was appropriate segregation of duties and that incompatible duties did not exist. Inquired with management and inspected the organizational chart to confirm that distinct system support functions were performed by different individuals, including the following: • IS management, • System design, • Application programming, • Systems programming, • Quality assurance/testing, • Library management/change management, • Computer operations, • Production control and scheduling, • Data control, • Data security, • Data administration, and • Network Administration.	**No relevant exceptions noted**

No.	Control Objective	Control Activity	Test Procedure	Results of Testing
63	System management job descriptions have been documented.	DFAS-Pensacola Developed position descriptions for distinct system support positions.	DFAS-Pensacola Inspected the job descriptions for the personnel who support DCPS.	**No relevant exceptions noted**
64	System management employees understand their duties and responsibilities.	DFAS-Pensacola Personnel receive and sign their position descriptions to confirm that they are aware of their proposed duties.	DFAS-Pensacola Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities. Observed documentation and confirmed that employees had signed position descriptions.	**No relevant exceptions noted**
65	Management reviews effectiveness of control techniques.	DFAS-Pensacola Management will periodically review and update security policies and procedures.	DFAS-Pensacola TSO Inspected the DCPS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each was periodically updated.	**No relevant exceptions noted**
66	Formal procedures guide system management personnel in performing their duties.	DFAS-Pensacola Formal SOPs for personnel who support DCPS.	DFAS-Pensacola Inspected SOPs used by personnel for performance of their job duties in respect to DCPS	**No relevant exceptions noted**
67	Access procedures enforce the principles of separation of duties and "least privilege."	DISA-Mechanicsburg and DFAS-Pensacola Privilege accounts are only used by DISA and DCPS personnel to create/modify/delete user accounts.	DISA-Mechanicsburg Inspected the access control policies and procedures for compliance with the principles of separation of duties and "least privilege." DFAS-Pensacola Inspected the access control policies and procedures for compliance with the principles of separation of duties and "least privilege."	**No relevant exceptions noted**
68				**Control objective left intentionally blank**

Section IV: Supplemental Information Provided by DFAS and DISA

IV. Supplemental Information Provided by DFAS and DISA

Introduction

This section has been prepared by DFAS and DISA and is included to provide user organizations with information DFAS and DISA believes will be of interest to such organizations; however, is not covered within the scope or control objectives established for the SAS 70 review. Specifically included is a summary of procedures that DFAS and DISA have put into place to enable recovery from a disaster affecting either DFAS TSOPE or DECC MECH.

This information has not been subjected to the procedures applied to the examination of the description of controls presented in Sections II and III of this report, and accordingly, the DoD OIG expresses no opinion regarding the completeness and accuracy of this information.

TSOPE Specific Business Continuity Plans

The DCPS production support Continuity of Operations Plan (COOP) provides an action plan to be implemented when there is a disaster or impending threat that would render DCPS production support inoperable (e.g., hurricane, damage to TSOPE facilities due to fire, etc.). This plan is evaluated and updated, accordingly, on an annual basis. If an impending threat or event occurs, production support control for the DCPS production support is transferred to an alternate-processing site, currently defined to be the Defense Ammunition Center Huntsville, AL. Contained in the detailed COOP are names of DCPS staff members who will serve as a pool of resources to be mobilized to execute the plan and a list of documentation and supplies that are necessary to support the mobilized team.

Team members are comprised of DCPS development staff members across many divisions and branches. TSOPE designates two members of the management team to be responsible for COOP execution. One is mobilized with the team and is responsible for team activities and communication with TSOPE while deployed to the COOP recovery site. The other serves as the team’s liaison at TSOPE and is responsible to relay current status, current area weather conditions, and other pertinent information to the mobilized team. The team is further divided into two teams, with each covering a 12-hour shift. Team leaders are appointed for the respective shift teams. Each step included in planning and executing the COOP is coordinated with full cooperation and involvement by the DCPS project management staff. Although this plan works for any type of disaster where production support becomes inoperable, it has been executed several times in the past few years during impending disastrous weather conditions, such as hurricanes.

DECC MECH Business Continuity Plans

To accommodate a major disaster at any major DISA processing center, DISA has established the DISA Continuity and Test Facility at Slidell, LA. This facility is equipped with computational, Direct Access Storage Devices, and telecommunications resources sized to provide a fully functional host site with the capacity to support a major disaster at any DISA processing center. The COOP support agreement between DFAS, as the customer, and DISA, as the provider of processing systems and communications services, provides for restoring host site processing in the event of a major disaster and the timely resolution of problems during other disruptions that adversely affect DCPS processing. The plan, as it relates to DCPS, details data restoration procedures for the MZF OS/390 operating system, the DCPS Integrated Database Management System, and related mid-tier servers and communication devices. Backup tapes containing the incremental daily and the complete weekly backups are rotated offsite to the Processing Element Chambersburg for storage on a predetermined schedule.

The Crisis Management Team at DECC MECH is responsible for declaring a disaster has occurred and initiating the Business Continuity Plan. The Crisis Management Team will then activate the following response teams: Communications Team, Recovery Coordination Team, Site Recovery Team, and the Crisis Support Team. Each team has a specific set of responsibilities defined in the Business Continuity Plan. The contact information for each individual on each team is also included in the Business Continuity Plan. The plan is required to be tested on an annual basis. TSOPE personnel participate in the yearly COOP test to ensure that the process works correctly and documentation is updated appropriately.

Acronyms and Abbreviations

ACF2	Access Control Facility 2
ACL	Access Control List
AIS	Automated Information System
CAC	Common Access Card
CCB	Configuration Control Board
CM	Configuration Management
CMIS	Change Management Information System
COOP	Continuity of Operations Plan
COTS	Commercial off-the shelf
CSR	Customer Service Representatives
DAC	Discretionary Access Control
DAPS	Defense Automated Printing Service
DCPS	Defense Civilian Pay System
DECC	Defense Enterprise Computing Center
DECC MECH	Defense Enterprise Computing Center Mechanicsburg
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DMI	Desktop Management Initiative
DMZ	Demilitarized Zones
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOD OIG	Department of Defense Office of Inspector General
DOE	Department of Energy
DPL	Director’s Policy Letter
EOP	Executive Office of the President
FSO	Field Security Operations
GOTS	Government off –the shelf
HHS	Department of Health and Human Service
IAVM	Information Assurance Vulnerability Management
IA	Information Assurance
ID	Identification
IP	Internet Protocol
IDMS	Integrated Database Management System
IDS	Intrusion Detection System
ISO	Information Security Officer

ISS	Information Security Scanner
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
LPAR	Logical Partition
M&CPS	Military & Civilian Pay Services
MAC	Mission Assurance Category
MOA	Memorandum of Agreement
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of the Inspector General
OLQ	Online Queries
OS	Operating System
SA	System Administrator
SAAR	Systems Access Authorization Request
SCR	System Change Request
SDLC	System Development Life Cycle
SMC	System Management Center
SMO	System Management Office
SNA	Systems Network Architecture
SOP	Standard Operating Procedures
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SSAA	System Security Authorization Agreement
SSN	Social Security Number
SSO	System Support Office
STIG	Security Technical Implementation Guide
TASO	Terminal Area Security Officer
TSO	Technology Services Organization
TSOPE	Technology Services Engineering Organization in Pensacola
TSP	Thrift Savings Plan
VMS	Vulnerability Management System
VPN	Virtual Private Network

Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
 Deputy Chief Financial Officer
 Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

Director, National Security Agency
Director, Defense Finance and Accounting Service
Inspector General, Defense Information Systems Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
General Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Members

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Team Members

The Defense Financial Auditing Service, Department of Defense Office of Inspector General, in conjunction with contract auditors from Acuity Consulting, Inc., produced this report. Personnel from the Technical Assessment Division and Quantitative Methods Division, Department of Defense Office of Inspector General, also contributed to the report.

Paul J. Granetto
Patricia A. Marsh
Addie M. Beima
Michael Perkins
Kenneth H. Stavenjord
Frank C. Sonsini
Sean J. Keaney
Anh H. Tran
Charles S. Dekle
Ernest G. Fine
Travis R. Schenck
Mary A. Hoover
Joey S. Sparks
Nicholas Drotar, Jr
Alberto J. Calimano-Colon
Jennifer K. Thorson